

LAW OFFICES  
**SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC**  
2100 PENNSYLVANIA AVENUE, N.W.  
WASHINGTON, DC 20037-3213  
TELEPHONE (202) 293-7060  
FACSIMILE (202) 293-7860  
www.sughrue.com

#2



April 20, 2001

BOX PATENT APPLICATION  
Commissioner for Patents  
Washington, D.C. 20231

Re: Application of Kazuyuki YOSHIDA, Yoshiaki MORIYAMA, Kazuo KURODA, and Toshio SUZUKI  
INFORMATION RECORDING APPARATUS AND METHOD, INFORMATION  
REPRODUCING APPARATUS AND METHOD, INFORMATION RECORDING  
MEDIUM AND PROGRAM INFORMATION RECORDING MEDIUM  
Our Ref. Q64192

Dear Sir:

Attached hereto is the application identified above including one-hundred and five (105) sheets of the specification, including the claims and abstract, twelve (12) sheets of drawings, PTO Form 1595, executed Declaration and Power of Attorney and Assignment.

The Government filing fee is calculated as follows:

Total claims	40	-	20	=	20	x	\$18.00	=	\$360.00
Independent claims	14	-	3	=	11	x	\$80.00	=	\$880.00
Base Fee									\$710.00

<b>TOTAL FILING FEE</b>	<b>\$1950.00</b>
Recordation of Assignment	\$40.00
<b>TOTAL FEE</b>	<b>\$1990.00</b>

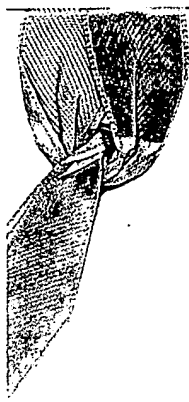
Checks for the statutory filing fee of \$1950.00 and Assignment recordation fee of \$40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from April 21, 2000, based on JP Application No. 2000-121636. The priority document is enclosed herewith.

Respectfully submitted,  
SUGHRUE, MION, ZINN,  
MACPEAK & SEAS, PLLC  
Attorneys for Applicant

By: Darryl Mexic  
Darryl Mexic  
Registration No. 23,063

DM:ob



日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

J1036 U.S. PTO  
09/838206  
04/20/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application: 2000年 4月21日

出 願 番 号  
Application Number: 特願2000-121636

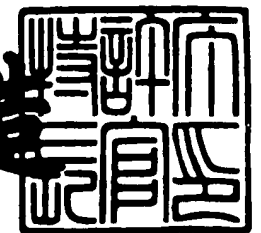
出 願 人  
Applicant (s): パイオニア株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 2月23日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 54P0688

【提出日】 平成12年 4月21日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/14  
H04L 9/28

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 吉田 和幸

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 守山 義明

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 黒田 和男

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 鈴木 敏雄

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【代理人】

【識別番号】 100083839

【弁理士】

【氏名又は名称】 石川 泰男

【電話番号】 03-5443-8461

【手数料の表示】

【予納台帳番号】 007191

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9102133

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録装置及び方法、情報再生装置及び方法並びに情報記録媒体

【特許請求の範囲】

【請求項 1】 記録情報を記録すべき情報記録媒体個々に固有の識別情報を用いて置換情報を生成する置換情報生成手段と、

前記記録情報の一部を前記生成された置換情報に置換し置換記録情報を生成する置換手段と、

前記生成された置換記録情報を、前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録手段と、

を備えることを特徴とする情報記録装置。

【請求項 2】 請求項 1 に記載の情報記録装置において、

予め設定された鍵情報を用いて前記記録情報を暗号化し、暗号化記録情報を生成する生成手段を更に備えると共に、

前記置換手段は、前記生成された暗号化記録情報の一部を前記生成された置換情報により置換して前記置換記録情報を生成し、

更に前記記録手段は、前記鍵情報を前記生成された置換記録情報と共に前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録することを特徴とする情報記録装置。

【請求項 3】 請求項 2 に記載の情報記録装置において、

前記置換情報生成手段は、前記鍵情報を含ませて前記置換情報を生成することを特徴とする情報記録装置。

【請求項 4】 請求項 2 又は 3 に記載の情報記録装置において、

前記識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する鍵情報暗号化手段を更に備え、

前記記録手段は、前記鍵情報に代えて前記生成された暗号化鍵情報を前記情報記録媒体に記録することを特徴とする情報記録装置。

【請求項 5】 請求項 4 に記載の情報記録装置において、

前記識別情報に対して予め設定された暗号化処理を施して当該識別情報を暗号

化し、暗号化識別情報を生成する識別情報暗号化手段を更に備え、

前記鍵情報暗号化手段は、前記生成された暗号化識別情報を用いて前記鍵情報を暗号化して前記暗号化鍵情報を生成することを特徴とする情報記録装置。

【請求項 6】 請求項 1 から 5 のいずれか一項に記載の情報記録装置において、

前記置換情報生成手段は、前記識別情報に対して予め設定された暗号化処理を施して得られる暗号化識別情報を用いて前記置換情報を生成することを特徴とする情報記録装置。

【請求項 7】 請求項 5 又は 6 に記載の情報記録装置において、

前記暗号化処理は、一方向性を有する予め設定された暗号化関数を用いて前記識別情報を暗号化する暗号化処理であることを特徴とする情報記録装置。

【請求項 8】 請求項 1 から 7 のいずれか一項に記載の情報記録装置において、

前記記録情報に対してエラー訂正用の訂正符号を付加し付加記録情報を生成する付加手段を更に備えると共に、

前記置換手段は、前記付加記録情報の一部を前記生成された置換情報に置換し、前記置換記録情報を生成することを特徴とする情報記録装置。

【請求項 9】 請求項 1 から 8 のいずれか一項に記載の情報記録装置において、

前記記録手段は、前記置換情報の生成に用いられた前記識別情報を、前記生成された置換記録情報と共に当該識別情報に対応する前記情報記録媒体に記録することを特徴とする情報記録装置。

【請求項 1 0】 請求項 1 から 8 のいずれか一項に記載の情報記録装置において、

前記識別情報は、対応する前記情報記録媒体に予め記録されていると共に、

前記置換情報生成手段は、当該記録されている識別情報を検出して前記置換情報の生成に用いることを特徴とする情報記録装置。

【請求項 1 1】 請求項 1 から 1 0 のいずれか一項に記載の情報記録装置において、

前記置換手段は、前記置換情報を用いた置換態様を、前記識別情報を用いて変更することを特徴とする情報記録装置。

【請求項 1 2】 予め設定された鍵情報を用いて情報記録媒体に記録すべき記録情報を暗号化し、暗号化記録情報を生成する生成手段と、

前記情報記録媒体に記録されている当該情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する暗号化鍵情報生成手段と

前記生成された暗号化記録情報及び前記生成された暗号化鍵情報を、当該暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録手段と、

を備えることを特徴とする情報記録装置。

【請求項 1 3】 請求項 1 2 に記載の情報記録装置において、

前記生成された暗号化記録情報の一部を前記生成された暗号化鍵情報に置換し置換記録情報を生成する置換手段を更に備え、

前記記録手段は、前記生成された置換記録情報を前記暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録することを特徴とする情報記録装置。

【請求項 1 4】 記録情報を記録すべき情報記録媒体個々に固有の識別情報を用いて生成された置換情報により前記記録情報の一部を置換して得られる置換記録情報が記録される情報記録領域と、

当該情報記録媒体に対応する前記識別情報が記録されている識別情報記録領域と、

を備えることを特徴とする情報記録媒体。

【請求項 1 5】 請求項 1 4 に記載の情報記録媒体において、

前記情報記録領域には、予め設定された鍵情報を用いて前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られる前記置換記録情報が記録されることを特徴とする情報記録媒体。

【請求項 1 6】 予め設定された鍵情報を用いて情報記録媒体に記録すべき記録情報を暗号化して得られる暗号化記録情報と、

前記情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、

が記録される情報記録領域と、

前記情報記録媒体に対応する前記識別情報が記録されている識別情報記録領域と、

を備えることを特徴とする情報記録媒体。

【請求項 1 7】 情報記録媒体個々に固有の識別情報を用いて生成された置換情報により記録情報の一部を置換して得られる置換記録情報が記録されていると共に、当該情報記録媒体に対応する前記識別情報が記録されている情報記録媒体から前記置換記録情報を検出する検出手段と、

当該情報記録媒体から前記識別情報を検出する識別情報検出手段と、

前記検出された置換記録情報から前記置換情報を抽出する置換情報抽出手段と

前記抽出された置換情報から前記識別情報を抽出する識別情報抽出手段と、

前記置換情報から抽出された識別情報と、前記情報記録媒体から検出された識別情報とを比較する比較手段と、

前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された置換記録情報から得られる前記記録情報の再生を行う再生手段と、

を備えることを特徴とする情報再生装置。

【請求項 1 8】 請求項 1 7 に記載の情報再生装置において、

前記置換記録情報は、予め設定された鍵情報により前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られていると共に、当該鍵情報及び前記得られた置換記録情報が前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録されており、

当該情報記録媒体から前記鍵情報を検出する鍵情報検出手段を更に備え、

前記再生手段は、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情



報を再生することを特徴とする情報再生装置。

【請求項 1 9】 請求項 1 8 に記載の情報再生装置において、  
前記鍵情報は前記置換情報内に含まれて前記情報記録媒体に記録されていると  
共に、

前記鍵情報検出手段は、前記抽出された置換情報内から前記鍵情報を検出する  
ことを特徴とする情報再生装置。

【請求項 2 0】 請求項 1 8 又は 1 9 に記載の情報再生装置において、  
前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報が当該鍵  
情報に代えて前記情報記録媒体に記録されていると共に、

前記鍵情報検出手段は、前記情報記録媒体から当該暗号化鍵情報を検出し、  
前記検出された識別情報を用いて当該検出された暗号化鍵情報を解読し、前記  
鍵情報を生成する鍵情報生成手段を更に備え、

前記再生手段は、前記置換情報から抽出された識別情報と前記情報記録媒体か  
ら検出された識別情報とが一致したときのみ、前記生成された鍵情報を用いて前  
記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情  
報を再生することを特徴とする情報再生装置。

【請求項 2 1】 請求項 2 0 に記載の情報再生装置において、  
前記識別情報に対して予め設定された暗号化処理を施して得られる暗号化識別  
情報を用いて前記鍵情報を暗号化して前記暗号化鍵情報が得られて前記情報記録  
媒体に記録されていると共に、

前記鍵情報生成手段は、前記検出された識別情報に対して前記暗号化処理を施  
して得られる前記暗号化識別情報を用いて前記検出された暗号化鍵情報を解読し  
て前記鍵情報を生成することを特徴とする情報再生装置。

【請求項 2 2】 請求項 2 1 に記載の情報再生装置において、  
前記暗号化処理は、一方向性を有する予め設定された暗号化関数を用いて暗号  
化する暗号化処理であることを特徴とする情報再生装置。

【請求項 2 3】 請求項 1 7 から 2 2 のいずれか一項に記載の情報再生装置  
において、

前記置換情報は、前記置換記録情報が記録されるべき前記情報記録媒体に対応

する前記識別情報に対して予め設定された暗号化処理を施して得られる暗号化識別情報を用いて生成されていると共に、

前記抽出された置換情報から前記暗号化識別情報を抽出し、当該暗号化処理に対応する解読処理により当該暗号化識別情報を解読し、前記識別情報を生成する識別情報生成手段を更に備え、

前記再生手段は、前記生成された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記記録情報を再生することを特徴とする情報再生装置。

【請求項 2 4】 請求項 1 7 から 2 2 のいずれか一項に記載の情報再生装置において、

前記置換情報は、前記置換記録情報が記録されるべき前記情報記録媒体に対応する前記識別情報に対して予め設定された一方向性を有する暗号化関数を用いた暗号化処理を施して得られる暗号化識別情報を用いて生成されていると共に、

前記抽出された置換情報から前記暗号化識別情報を抽出する暗号化識別情報抽出手段と、

前記検出された識別情報に対して前記暗号化関数を用いた前記暗号化処理を施し、副暗号化識別情報を生成する暗号化識別情報生成手段と、

を更に備え、

前記再生手段は、前記生成された副暗号化識別情報と前記抽出された暗号化識別情報とが一致したときのみ、前記記録情報を再生することを特徴とする情報再生装置。

【請求項 2 5】 請求項 1 7 から 2 4 のいずれか一項に記載の情報再生装置において、

前記置換記録情報は前記記録情報に対してエラー訂正用の訂正符号を付加して生成される付加記録情報の一部を前記生成された置換情報に置換して生成され前記情報記録媒体に記録されていると共に、

前記置換情報抽出手段は、エラー訂正前の前記置換記録情報から前記置換情報を抽出し、

前記検出された置換記録情報に対して前記訂正符号を用いたエラー訂正処理を

施す訂正手段を更に備えることを特徴とする情報再生装置。

【請求項 2 6】 請求項 1 7 から 2 5 のいずれか一項に記載の情報再生装置において、

前記置換記録情報における前記置換情報による置換態様が前記識別情報を用いて変更されていると共に、

前記置換情報抽出手段は、前記検出された識別情報を用いて特定される前記置換態様に基づいて前記検出された置換記録情報から前記置換情報を抽出することを特徴とする情報再生装置。

【請求項 2 7】 情報記録媒体個々に固有の識別情報が記録されている当該情報記録媒体に記録すべき記録情報を予め設定された鍵情報を用いて暗号化して得られる暗号化記録情報と、前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録されている前記情報記録媒体から前記暗号化記録情報及び前記暗号化鍵情報を検出する検出手段と、

当該情報記録媒体から前記識別情報を検出する識別情報検出手段と、

前記検出された暗号化鍵情報を前記検出された識別情報を用いて解読し、前記鍵情報を生成する鍵情報生成手段と、

前記生成された鍵情報を用いて前記検出された暗号化記録情報を解読して再生する再生手段と、

を備えることを特徴とする情報再生装置。

【請求項 2 8】 請求項 2 7 に記載の情報再生装置において、

前記生成された暗号化記録情報の一部が前記生成された暗号化鍵情報により置換して生成された置換記録情報が前記情報記録媒体に記録されていると共に、

前記検出手段は前記情報記録媒体から当該置換記録情報を検出し、

前記検出された置換記録情報から前記暗号化鍵情報を抽出する鍵情報抽出手段を更に備えることを特徴とする情報再生装置。

【請求項 2 9】 記録情報を記録すべき情報記録媒体個々に固有の識別情報を用いて置換情報を生成する置換情報生成工程と、

前記記録情報の一部を前記生成された置換情報に置換し置換記録情報を生成する置換工程と、

前記生成された置換記録情報を、前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録工程と、

を備えることを特徴とする情報記録方法。

【請求項 3 0】 請求項 2 9 に記載の情報記録方法において、

予め設定された鍵情報を用いて前記記録情報を暗号化し、暗号化記録情報を生成する生成工程を更に備えると共に、

前記置換工程においては、前記生成された暗号化記録情報の一部を前記生成された置換情報により置換して前記置換記録情報を生成し、

更に前記記録工程においては、前記鍵情報を前記生成された置換記録情報と共に前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録することを特徴とする情報記録方法。

【請求項 3 1】 予め設定された鍵情報を用いて情報記録媒体に記録すべき記録情報を暗号化し、暗号化記録情報を生成する生成工程と、

前記情報記録媒体に記録されている当該情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する暗号化鍵情報生成工程と、

前記生成された暗号化記録情報及び前記生成された暗号化鍵情報を、当該暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録工程と、

を備えることを特徴とする情報記録方法。

【請求項 3 2】 情報記録媒体個々に固有の識別情報を用いて生成された置換情報により記録情報の一部を置換して得られる置換記録情報が記録されていると共に、当該情報記録媒体に対応する前記識別情報が記録されている情報記録媒体から前記置換記録情報を検出する検出工程と、

当該情報記録媒体から前記識別情報を検出する識別情報検出工程と、

前記検出された置換記録情報から前記置換情報を抽出する置換情報抽出工程と、

前記抽出された置換情報から前記識別情報を抽出する識別情報抽出工程と、

前記置換情報から抽出された識別情報と、前記情報記録媒体から検出された識

別情報とを比較する比較工程と、

前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された置換記録情報から得られる前記記録情報の再生を行う再生工程と、

を備えることを特徴とする情報再生方法。

【請求項 3 3】 請求項 3 2 に記載の情報再生方法において、

前記置換記録情報は、予め設定された鍵情報により前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られていると共に、当該鍵情報及び前記得られた置換記録情報が前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録されており、

当該情報記録媒体から前記鍵情報を検出する鍵情報検出工程を更に備え、

前記再生工程においては、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情報を再生することを特徴とする情報再生方法。

【請求項 3 4】 情報記録媒体個々に固有の識別情報が記録されている当該情報記録媒体に記録すべき記録情報を予め設定された鍵情報を用いて暗号化して得られる暗号化記録情報と、前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録されている前記情報記録媒体から前記暗号化記録情報及び前記暗号化鍵情報を検出する検出工程と、

当該情報記録媒体から前記識別情報を検出する識別情報検出工程と、

前記検出された暗号化鍵情報を前記検出された識別情報を用いて解読し、前記鍵情報を生成する鍵情報生成工程と、

前記生成された鍵情報を用いて前記検出された暗号化記録情報を解読して再生する再生工程と、

を備えることを特徴とする情報再生方法。

【請求項 3 5】 記録情報を情報記録媒体に記録する情報記録装置に含まれるコンピュータを、

記録情報を記録すべき情報記録媒体個々に固有の識別情報を用いて置換情報を

生成する置換情報生成手段、

前記記録情報の一部を前記生成された置換情報に置換し置換記録情報を生成する置換手段、及び、

前記生成された置換記録情報を、前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録手段、

として機能させることを特徴とする情報記録制御プログラムが前記コンピュータで読取可能に記録された情報記録媒体。

【請求項 3 6】 請求項 3 5 に記載の情報記録媒体において、

前記コンピュータを、予め設定された鍵情報を用いて前記記録情報を暗号化し、暗号化記録情報を生成する生成手段として更に機能させると共に、

前記置換手段として機能する前記コンピュータを、前記生成された暗号化記録情報の一部を前記生成された置換情報により置換して前記置換記録情報を生成するように機能させ、

更に前記記録手段として機能する前記コンピュータを、前記鍵情報を前記生成された置換記録情報と共に前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録するように機能させることを特徴とする前記情報記録制御プログラムが前記コンピュータで読取可能に記録された情報記録媒体。

【請求項 3 7】 記録情報を情報記録媒体に記録する情報記録装置に含まれるコンピュータを、

予め設定された鍵情報を用いて情報記録媒体に記録すべき記録情報を暗号化し、暗号化記録情報を生成する生成手段、

前記情報記録媒体に記録されている当該情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する暗号化鍵情報生成手段、及び、

前記生成された暗号化記録情報及び前記生成された暗号化鍵情報を、当該暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録手段、

として機能させることを特徴とする情報記録制御プログラムが前記コンピュータで読取可能に記録された情報記録媒体。

【請求項 3 8】 情報再生装置に含まれているコンピュータを、

情報記録媒体個々に固有の識別情報を用いて生成された置換情報により記録情報の一部を置換して得られる置換記録情報が記録されていると共に、当該情報記録媒体に対応する前記識別情報が記録されている情報記録媒体から前記置換記録情報を検出する検出手段、

当該情報記録媒体から前記識別情報を検出する識別情報検出手段、

前記検出された置換記録情報から前記置換情報を抽出する置換情報抽出手段、

前記抽出された置換情報から前記識別情報を抽出する識別情報抽出手段、

前記置換情報から抽出された識別情報と、前記情報記録媒体から検出された識別情報とを比較する比較手段、及び、

前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された置換記録情報から得られる前記記録情報の再生を行う再生手段、

として機能させることを特徴とする情報再生制御プログラムが前記コンピュータで読取可能に記録された情報記録媒体。

【請求項 3 9】 請求項 3 8 に記載の情報記録媒体において、

前記置換記録情報は、予め設定された鍵情報により前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られていると共に、当該鍵情報及び前記得られた置換記録情報が前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録されており、

前記コンピュータを、当該情報記録媒体から前記鍵情報を検出する鍵情報検出手段として更に機能させると共に、

前記再生手段として機能する前記コンピュータを、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情報を再生するように機能させることを特徴とする前記情報再生制御プログラムが前記コンピュータで読取可能に記録された情報記録媒体。

【請求項 4 0】 情報再生装置に含まれるコンピュータを、

情報記録媒体個々に固有の識別情報が記録されている当該情報記録媒体に記録すべき記録情報を予め設定された鍵情報を用いて暗号化して得られる暗号化記録情報と、前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録されている前記情報記録媒体から前記暗号化記録情報及び前記暗号化鍵情報を検出する検出手段、

当該情報記録媒体から前記識別情報を検出する識別情報検出手段、

前記検出された暗号化鍵情報を前記検出された識別情報を用いて解読し、前記鍵情報を生成する鍵情報生成手段、及び、

前記生成された鍵情報を用いて前記検出された暗号化記録情報を解読して再生する再生手段、

として機能させることを特徴とする情報再生制御プログラムが前記コンピュータで読取可能に記録された情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報記録装置及び方法、情報再生装置及び方法並びに情報記録媒体の技術分野に属し、より詳細には、光ディスク等の情報記録媒体に対して画像情報等の記録情報を記録するための情報記録装置及び方法、当該情報記録装置等により記録情報が記録された情報記録媒体並びに当該情報記録媒体から記録情報を再生するための情報再生装置及び方法並びに当該情報記録又は情報再生のための制御プログラムがコンピュータで読取可能に記録された情報記録媒体の技術分野に属する。

【0002】

【従来の技術】

一般的に映画等のビデオ情報や音楽等のオーディオ情報は著作権により保護されている場合が多く、その場合には、これらの情報を無断で複製すること及び当該無断複製された情報を再生することは原則として禁止されている。

【0003】

また、当該著作権者においては、これらの無断複製及びその再生を効果的に防



止する方策を取る必要がある。

【0004】

ここで、従来の不法複写防止方法として、上記ビデオ情報等の中に当該ビデオ情報の複写記録の回数を制限するための制限情報を重畳して情報記録媒体に記録しておき、当該ビデオ情報の再生及び複写記録時においてその制限情報に基づいて複写を制限することで、許可されない複写記録を防止する構成がとられる場合がある。

【0005】

このとき、当該制限情報を用いた無断複写防止方法についてより具体的には、例えば、一回のみ複写記録を許可する旨の制限情報と共にビデオ情報等を情報記録媒体に記録し、次に、当該記録されているビデオ情報等を再生して他の情報記録媒体に複写記録する際に当該一回のみ複写記録を許可する旨の制限情報を以後の複写記録を禁止する旨の制限情報に変更してビデオ情報等に重畳して複写記録するようにすれば、当該他の情報記録媒体からビデオ情報等を読み出して再度複写記録しようとしても、それには複写記録禁止を示す制限情報が重畳されているので、当該他の情報記録媒体からの複写記録は実行不可能となるのである。

【0006】

【発明が解決しようとする課題】

しかしながら、上述のような制限情報を用いた無断複写防止方法によると、一回のみ複写記録を許可する旨の制限情報が重畳されたビデオ情報等が記録されている情報記録媒体から当該ビデオ情報等を復号せずに当該記録されている形のままで（すなわち、いわゆるRF（Radio Frequency）信号のままで）他の情報記録媒体に不法複写された場合には、当該制限情報も一回のみ複写記録を許可する旨の内容のまま当該他の情報記録媒体に不法複写されるので、結果として当該他の情報記録媒体からの更なる複写が可能となり、無断複写を有効に禁止することができない場合があるという問題点があった。

【0007】

そこで、本発明は、上記の問題点に鑑みて為されたもので、その課題は、ビデオ情報等が復号されずに当該情報記録媒体に記録されている形のままで他の情報

記録媒体に不法複写された場合でも、当該不法複写された記録情報が再生されることを防止することが可能な状態でビデオ情報等を当該情報記録媒体に記録することが可能な情報記録装置及び方法、当該情報記録装置等によりビデオ情報等が記録された情報記録媒体並びに当該情報記録媒体からビデオ情報等を再生するための情報再生装置及び方法並びに当該情報記録又は情報再生のための制御プログラムがコンピュータで読取可能に記録された情報記録媒体を提供することにある。

## 【 0 0 0 8 】

## 【課題を解決するための手段】

上記の課題を解決するために、請求項 1 に記載の発明は、記録情報を記録すべき DVD 等の情報記録媒体個々に固有の識別情報を用いて置換情報を生成する置換情報生成器等の置換情報生成手段と、前記記録情報の一部を前記生成された置換情報に置換し置換記録情報を生成する置換情報書込器等の置換手段と、前記生成された置換記録情報を、前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する光変調器等の記録手段と、を備える。

## 【 0 0 0 9 】

よって、情報記録媒体に記録される置換記録情報が当該情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録されている置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらに対応関係を有している場合にのみ再生を許可することで、不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 1 0 】

上記の課題を解決するために、請求項 2 に記載の発明は、請求項 1 に記載の情報記録装置において、予め設定された鍵情報を用いて前記記録情報を暗号化し、暗号化記録情報を生成するデータ暗号化器等の生成手段を更に備えると共に、前記置換手段は、前記生成された暗号化記録情報の一部を前記生成された置換情報により置換して前記置換記録情報を生成し、更に前記記録手段は、前記鍵情報を

前記生成された置換記録情報と共に前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録するように構成される。

【 0 0 1 1 】

よって、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に有効に防止できる。

【 0 0 1 2 】

上記の課題を解決するために、請求項 3 に記載の発明は、請求項 2 に記載の情報記録装置において、前記置換情報生成手段は、前記鍵情報を含ませて前記置換情報を生成するように構成される。

【 0 0 1 3 】

よって、再生時における鍵情報の取得がより困難となり、不法複写された記録情報の再生を更に困難とすることができる。

【 0 0 1 4 】

上記の課題を解決するために、請求項 4 に記載の発明は、請求項 2 又は 3 に記載の情報記録装置において、前記識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する置換情報生成器等の鍵情報暗号化手段を更に備え、前記記録手段は、前記鍵情報に代えて前記生成された暗号化鍵情報を前記情報記録媒体に記録するように構成される。

【 0 0 1 5 】

よって、再生時における不法な鍵情報の取得及びそれを用いた記録情報の復号を防止できる。

【 0 0 1 6 】

上記の課題を解決するために、請求項 5 に記載の発明は、請求項 4 に記載の情報記録装置において、前記識別情報に対して予め設定された暗号化処理を施して当該識別情報を暗号化し、暗号化識別情報を生成する置換情報生成器等の識別情報暗号化手段を更に備え、前記鍵情報暗号化手段は、前記生成された暗号化識別情報を用いて前記鍵情報を暗号化して前記暗号化鍵情報を生成するように構成される。

【 0 0 1 7 】

よって、記録情報を復号するための鍵情報が当該再生時において不法に取得されることを困難とすることができる。

【 0 0 1 8 】

上記の課題を解決するために、請求項 6 に記載の発明は、請求項 1 から 5 のいずれか一項に記載の情報記録装置において、前記置換情報生成手段は、前記識別情報に対して予め設定された暗号化処理を施して得られる暗号化識別情報を用いて前記置換情報を生成するように構成される。

【 0 0 1 9 】

よって、置換記録情報との比較対象となる識別情報が再生時において不法に取得されることを困難とすることができる。

【 0 0 2 0 】

上記の課題を解決するために、請求項 7 に記載の発明は、請求項 5 又は 6 に記載の情報記録装置において、前記暗号化処理は、一方向性を有する予め設定された暗号化関数を用いて前記識別情報を暗号化する暗号化処理であるように構成される。

【 0 0 2 1 】

よって、再生時における識別情報の取得を更に困難とすることができる。

【 0 0 2 2 】

上記の課題を解決するために、請求項 8 に記載の発明は、請求項 1 から 7 のいずれか一項に記載の情報記録装置において、前記記録情報に対してエラー訂正用の訂正符号を付加し付加記録情報を生成する ECC エンコーダ等の付加手段を更に備えると共に、前記置換手段は、前記付加記録情報の一部を前記生成された置換情報に置換し、前記置換記録情報を生成するように構成される。

【 0 0 2 3 】

よって、再生時において正確に記録情報を再生することができる。

【 0 0 2 4 】

上記の課題を解決するために、請求項 9 に記載の発明は、請求項 1 から 8 のいずれか一項に記載の情報記録装置において、前記記録手段は、前記置換情報の生成に用いられた前記識別情報を、前記生成された置換記録情報と共に当該識別情

報に対応する前記情報記録媒体に記録するように構成される。

【 0 0 2 5 】

よって、置換記録情報と共に記録された識別情報と当該置換記録情報の内容とをその再生時に比較することで、正規に記録された置換記録情報のみを再生可能とすることができる。

【 0 0 2 6 】

上記の課題を解決するために、請求項 1 0 に記載の発明は、請求項 1 から 8 のいずれか一項に記載の情報記録装置において、前記識別情報は、対応する前記情報記録媒体に予め記録されていると共に、前記置換情報生成手段は、当該記録されている識別情報を検出して前記置換情報の生成に用いるように構成される。

【 0 0 2 7 】

よって、予め記録されている識別情報と当該置換記録情報の内容とをその再生時に比較することで、正規に記録された置換記録情報のみを再生可能とすることができる。

【 0 0 2 8 】

上記の課題を解決するために、請求項 1 1 に記載の発明は、請求項 1 から 1 0 のいずれか一項に記載の情報記録装置において、前記置換手段は、前記置換情報を用いた置換態様を、前記識別情報を用いて変更するように構成される。

【 0 0 2 9 】

よって、当該置換態様が識別情報により変更されているので、不法複写された記録情報の再生を更に困難にすることができる。

【 0 0 3 0 】

上記の課題を解決するために、請求項 1 2 に記載の発明は、予め設定された鍵情報を用いて D V D 等の情報記録媒体に記録すべき記録情報を暗号化し、暗号化記録情報を生成するデータ暗号化器等の生成手段と、前記情報記録媒体に記録されている当該情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する置換情報生成器等の暗号化鍵情報生成手段と、前記生成された暗号化記録情報及び前記生成された暗号化鍵情報を、当該暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する光変調

器等の記録手段と、を備える。

【 0 0 3 1 】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

【 0 0 3 2 】

上記の課題を解決するために、請求項 1 3 に記載の発明は、請求項 1 2 に記載の情報記録装置において、前記生成された暗号化記録情報の一部を前記生成された暗号化鍵情報に置換し置換記録情報を生成する置換手段を更に備え、前記記録手段は、前記生成された置換記録情報を前記暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録するように構成される。

【 0 0 3 3 】

よって、暗号化記録情報の一部が暗号化鍵情報とされるので、再生時における当該暗号化鍵情報の取得を困難とすることができる。

【 0 0 3 4 】

上記の課題を解決するために、請求項 1 4 に記載の発明は、記録情報を記録すべき DVD 等の情報記録媒体個々に固有の識別情報を用いて生成された置換情報により前記記録情報の一部を置換して得られる置換記録情報が記録される情報記録領域と、当該情報記録媒体に対応する前記識別情報が記録されている識別情報記録領域と、を備える。

【 0 0 3 5 】

よって、記録される置換記録情報が情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録される置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらに対応関係を有

している場合にのみ再生を許可することで、情報記録媒体に不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 3 6 】

上記の課題を解決するために、請求項 1 5 に記載の発明は、請求項 1 4 に記載の情報記録媒体において、前記情報記録領域には、予め設定された鍵情報を用いて前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られる前記置換記録情報が記録されるように構成される。

## 【 0 0 3 7 】

よって、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に防止できる。

## 【 0 0 3 8 】

上記の課題を解決するために、請求項 1 6 に記載の発明は、予め設定された鍵情報を用いて情報記録媒体に記録すべき記録情報を暗号化して得られる暗号化記録情報と、前記情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録される情報記録領域と、前記情報記録媒体に対応する前記識別情報が記録されている識別情報記録領域と、を備える。

## 【 0 0 3 9 】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 4 0 】

上記の課題を解決するために、請求項 1 7 に記載の発明は、情報記録媒体個々に固有の識別情報を用いて生成された置換情報により記録情報の一部を置換して

得られる置換記録情報が記録されていると共に、当該情報記録媒体に対応する前記識別情報が記録されている情報記録媒体から前記置換記録情報を検出するピックアップ等の検出手段と、当該情報記録媒体から前記識別情報を検出するピックアップ等の識別情報検出手段と、前記検出された置換記録情報から前記置換情報を抽出する置換情報抽出器等の置換情報抽出手段と、前記抽出された置換情報から前記識別情報を抽出する識別情報抽出器等の識別情報抽出手段と、前記置換情報から抽出された識別情報と、前記情報記録媒体から検出された識別情報とを比較する識別情報比較器等の比較手段と、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された置換記録情報から得られる前記記録情報の再生を行う出力制御器等の再生手段と、を備える。

## 【 0 0 4 1 】

よって、情報記録媒体に記録されている置換記録情報が当該情報記録媒体に対応する識別情報毎に異なっていることにより当該置換記録情報が情報記録媒体個々に異なっていると共に、検出された置換記録情報と検出された識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された（すなわち、検出された識別情報と記録されている置換記録情報とが一致しない形で記録された）記録情報が再生されることを未然に防止できる。

## 【 0 0 4 2 】

上記の課題を解決するために、請求項 1 8 に記載の発明は、請求項 1 7 に記載の情報再生装置において、前記置換記録情報は、予め設定された鍵情報により前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られていると共に、当該鍵情報及び前記得られた置換記録情報が前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録されており、当該情報記録媒体から前記鍵情報を検出するピックアップ等の鍵情報検出手段を更に備え、前記再生手段は、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情報を再生するように構成される。



【 0 0 4 3 】

よって、記録情報が暗号化されて記録されていると共に、これを検出された鍵情報を用いて再生するので、不法複写された記録情報の再生を更に有効に防止できる。

【 0 0 4 4 】

上記の課題を解決するために、請求項 1 9 に記載の発明は、請求項 1 8 に記載の情報再生装置において、前記鍵情報は前記置換情報内に含まれて前記情報記録媒体に記録されていると共に、前記鍵情報検出手段は、前記抽出された置換情報内から前記鍵情報を検出するように構成される。

【 0 0 4 5 】

よって、再生時における鍵情報の取得がより困難となり、不法複写された暗号化記録情報の解読・再生を更に困難とすることができる。

【 0 0 4 6 】

上記の課題を解決するために、請求項 2 0 に記載の発明は、請求項 1 8 又は 1 9 に記載の情報再生装置において、前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報が当該鍵情報に代えて前記情報記録媒体に記録されていると共に、前記鍵情報検出手段は、前記情報記録媒体から当該暗号化鍵情報を検出し、前記検出された識別情報を用いて当該検出された暗号化鍵情報を解読し、前記鍵情報を生成する置換情報抽出器等の鍵情報生成手段を更に備え、前記再生手段は、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記生成された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情報を再生するように構成される。

【 0 0 4 7 】

よって、記録情報の暗号化の解読に用いられる鍵情報の取得及びそれを用いた記録情報の復号を防止できる。

【 0 0 4 8 】

上記の課題を解決するために、請求項 2 1 に記載の発明は、請求項 2 0 に記載の情報再生装置において、前記識別情報に対して予め設定された暗号化処理を施

して得られる暗号化識別情報を用いて前記鍵情報を暗号化して前記暗号化鍵情報が得られて前記情報記録媒体に記録されていると共に、前記鍵情報生成手段は、前記検出された識別情報に対して前記暗号化処理を施して得られる前記暗号化識別情報を用いて前記検出された暗号化鍵情報を解読して前記鍵情報を生成するように構成される。

【0049】

よって、記録情報を復号するための鍵情報が当該再生時において不法に取得されることを更に困難とすることができる。

【0050】

上記の課題を解決するために、請求項22に記載の発明は、請求項21に記載の情報再生装置において、前記暗号化処理は、一方向性を有する予め設定された暗号化関数を用いて暗号化する暗号化処理であるように構成される。

【0051】

よって、暗号化鍵情報を解読するための暗号化識別情報の不法取得を更に困難とすることができる。

【0052】

上記の課題を解決するために、請求項23に記載の発明は、請求項17から22のいずれか一項に記載の情報再生装置において、前記置換情報は、前記置換記録情報が記録されるべき前記情報記録媒体に対応する前記識別情報に対して予め設定された暗号化処理を施して得られる暗号化識別情報を用いて生成されていると共に、前記抽出された置換情報から前記暗号化識別情報を抽出し、当該暗号化処理に対応する解読処理により当該暗号化識別情報を解読し、前記識別情報を生成する置換情報抽出器等の識別情報生成手段を更に備え、前記再生手段は、前記生成された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記記録情報を再生するように構成される。

【0053】

よって、情報記録媒体から検出された識別情報との比較対象となる識別情報を不法取得を更に困難とすることができる。

【0054】

上記の課題を解決するために、請求項 2 4 に記載の発明は、請求項 1 7 から 2 2 のいずれか一項に記載の情報再生装置において、前記置換情報は、前記置換記録情報が記録されるべき前記情報記録媒体に対応する前記識別情報に対して予め設定された一方向性を有する暗号化関数を用いた暗号化処理を施して得られる暗号化識別情報を用いて生成されていると共に、前記抽出された置換情報から前記暗号化識別情報を抽出する置換情報復号器等の暗号化識別情報抽出手段と、前記検出された識別情報に対して前記暗号化関数を用いた前記暗号化処理を施し、副暗号化識別情報を生成する置換情報復号器等の暗号化識別情報生成手段と、を更に備え、前記再生手段は、前記生成された副暗号化識別情報と前記抽出された暗号化識別情報とが一致したときのみ、前記記録情報を再生するように構成される。

## 【 0 0 5 5 】

よって、抽出された暗号化識別情報と生成された副暗号化識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された記録情報が再生されることを未然に防止できる。

## 【 0 0 5 6 】

上記の課題を解決するために、請求項 2 5 に記載の発明は、請求項 1 7 から 2 4 のいずれか一項に記載の情報再生装置において、前記置換記録情報は前記記録情報に対してエラー訂正用の訂正符号を付加して生成される付加記録情報の一部を前記生成された置換情報に置換して生成され前記情報記録媒体に記録されていると共に、前記置換情報抽出手段は、エラー訂正前の前記置換記録情報から前記置換情報を抽出し、前記検出された置換記録情報に対して前記訂正符号を用いたエラー訂正処理を施すエラー訂正回路等の訂正手段を更に備える。

## 【 0 0 5 7 】

よって、正確にエラー訂正を行って記録情報を再生することができる。

## 【 0 0 5 8 】

上記の課題を解決するために、請求項 2 6 に記載の発明は、請求項 1 7 から 2 5 のいずれか一項に記載の情報再生装置において、前記置換記録情報における前記置換情報による置換態様が前記識別情報を用いて変更されていると共に、前記

置換情報抽出手段は、前記検出された識別情報を用いて特定される前記置換態様に基づいて前記検出された置換記録情報から前記置換情報を抽出するように構成される。

## 【 0 0 5 9 】

よって、当該置換態様が識別情報毎に異なることとなっており、これを検出された識別情報により特定して再生するので、不法複写された記録情報の再生を更に困難にすることができる。

## 【 0 0 6 0 】

上記の課題を解決するために、請求項 2 7 に記載の発明は、DVD 等の情報記録媒体個々に固有の識別情報が記録されている当該情報記録媒体に記録すべき記録情報を予め設定された鍵情報を用いて暗号化して得られる暗号化記録情報と、前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録されている前記情報記録媒体から前記暗号化記録情報及び前記暗号化鍵情報を検出するピックアップ等の検出手段と、当該情報記録媒体から前記識別情報を検出するピックアップ等の識別情報検出手段と、前記検出された暗号化鍵情報を前記検出された識別情報を用いて解読し、前記鍵情報を生成する置換情報復号器等の鍵情報生成手段と、前記生成された鍵情報を用いて前記検出された暗号化記録情報を解読して再生するデータ復号器等の再生手段と、を備える。

## 【 0 0 6 1 】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されており、検出された識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生するので、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ鍵情報が取得できず、結果として記録情報の解読・再生ができないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 6 2 】

上記の課題を解決するために、請求項 2 8 に記載の発明は、請求項 2 7 に記載の情報再生装置において、前記生成された暗号化記録情報の一部が前記生成され

た暗号化鍵情報により置換して生成された置換記録情報が前記情報記録媒体に記録されていると共に、前記検出手段は前記情報記録媒体から当該置換記録情報を検出し、前記検出された置換記録情報から前記暗号化鍵情報を抽出する置換情報復号器等の鍵情報抽出手段を更に備える。

## 【 0 0 6 3 】

よって、暗号化鍵情報の取得をより困難として、不法複写された暗号化記録情報の解読・再生を防止することができる。

## 【 0 0 6 4 】

上記の課題を解決するために、請求項 2 9 に記載の発明は、記録情報を記録すべき DVD 等の情報記録媒体個々に固有の識別情報を用いて置換情報を生成する置換情報生成工程と、前記記録情報の一部を前記生成された置換情報に置換し置換記録情報を生成する置換工程と、前記生成された置換記録情報を、前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録工程と、を備える。

## 【 0 0 6 5 】

よって、情報記録媒体に記録される置換記録情報が当該情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録されている置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらに対応関係を有している場合にのみ再生を許可することで、不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 6 6 】

上記の課題を解決するために、請求項 3 0 に記載の発明は、請求項 2 9 に記載の情報記録方法において、予め設定された鍵情報を用いて前記記録情報を暗号化し、暗号化記録情報を生成する生成工程を更に備えると共に、前記置換工程においては、前記生成された暗号化記録情報の一部を前記生成された置換情報により置換して前記置換記録情報を生成し、更に前記記録工程においては、前記鍵情報を前記生成された置換記録情報と共に前記置換情報の生成に用いられた前記識別

情報に対応する前記情報記録媒体に記録するように構成される。

【0067】

よって、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に防止できる。

【0068】

上記の課題を解決するために、請求項31に記載の発明は、予め設定された鍵情報を用いてDVD等の情報記録媒体に記録すべき記録情報を暗号化し、暗号化記録情報を生成する生成工程と、前記情報記録媒体に記録されている当該情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する暗号化鍵情報生成工程と、前記生成された暗号化記録情報及び前記生成された暗号化鍵情報を、当該暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録工程と、を備える。

【0069】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

【0070】

上記の課題を解決するために、請求項32に記載の発明は、DVD等の情報記録媒体個々に固有の識別情報を用いて生成された置換情報により記録情報の一部を置換して得られる置換記録情報が記録されていると共に、当該情報記録媒体に対応する前記識別情報が記録されている情報記録媒体から前記置換記録情報を検出する検出工程と、当該情報記録媒体から前記識別情報を検出する識別情報検出工程と、前記検出された置換記録情報から前記置換情報を抽出する置換情報抽出工程と、前記抽出された置換情報から前記識別情報を抽出する識別情報抽出工程と、前記置換情報から抽出された識別情報と、前記情報記録媒体から検出された

識別情報とを比較する比較工程と、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された置換記録情報から得られる前記記録情報の再生を行う再生工程と、を備える。

## 【 0 0 7 1 】

よって、情報記録媒体に記録されている置換記録情報が当該情報記録媒体に対応する識別情報毎に異なっていることにより当該置換記録情報が情報記録媒体個々に異なっていると共に、検出された置換記録情報と検出された識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された（すなわち、検出された識別情報と記録されている置換記録情報とが一致しない形で記録された）記録情報が再生されることを未然に防止できる。

## 【 0 0 7 2 】

上記の課題を解決するために、請求項 3 3 に記載の発明は、請求項 3 2 に記載の情報再生方法において、前記置換記録情報は、予め設定された鍵情報により前記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られていると共に、当該鍵情報及び前記得られた置換記録情報が前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録されており、当該情報記録媒体から前記鍵情報を検出する鍵情報検出工程を更に備え、前記再生工程においては、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情報を再生するように構成される。

## 【 0 0 7 3 】

よって、記録情報が暗号化されて記録されていると共に、これを検出された鍵情報を用いて再生するので、不法複写された記録情報の再生を更に有効に防止できる。

## 【 0 0 7 4 】

上記の課題を解決するために、請求項 3 4 に記載の発明は、DVD等の情報記録媒体個々に固有の識別情報が記録されている当該情報記録媒体に記録すべき記録情報を予め設定された鍵情報を用いて暗号化して得られる暗号化記録情報と、

前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録されている前記情報記録媒体から前記暗号化記録情報及び前記暗号化鍵情報を検出する検出工程と、当該情報記録媒体から前記識別情報を検出する識別情報検出工程と、前記検出された暗号化鍵情報を前記検出された識別情報を用いて解読し、前記鍵情報を生成する鍵情報生成工程と、前記生成された鍵情報を用いて前記検出された暗号化記録情報を解読して再生する再生工程と、を備える。

## 【 0 0 7 5 】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されており、検出された識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生するので、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ鍵情報が取得できず、結果として記録情報の解読・再生ができないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 7 6 】

上記の課題を解決するために、請求項 3 5 に記載の発明は、記録情報を DVD 等の情報記録媒体に記録する情報記録装置に含まれるコンピュータを、記録情報を記録すべき情報記録媒体個々に固有の識別情報を用いて置換情報を生成する置換情報生成手段、前記記録情報の一部を前記生成された置換情報に置換し置換記録情報を生成する置換手段、前記生成された置換記録情報を、前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録手段、として機能させるための情報記録制御プログラムが前記コンピュータで読取可能に記録されている。

## 【 0 0 7 7 】

よって、情報記録媒体に記録される置換記録情報が当該情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録されている置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらに対応関係を有している場合にのみ再生を許可することで、不法複写さ



れた（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 0 7 8 】

上記の課題を解決するために、請求項 3 6 に記載の発明は、請求項 3 5 に記載の情報記録媒体において、前記コンピュータを、予め設定された鍵情報を用いて前記記録情報を暗号化し、暗号化記録情報を生成する生成手段として更に機能させると共に、前記置換手段として機能する前記コンピュータを、前記生成された暗号化記録情報の一部を前記生成された置換情報により置換して前記置換記録情報を生成するように機能させ、更に前記記録手段として機能する前記コンピュータを、前記鍵情報を前記生成された置換記録情報と共に前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録するように機能させるための前記情報記録制御プログラムが前記コンピュータで読取可能に記録されている。

## 【 0 0 7 9 】

よって、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に防止できる。

## 【 0 0 8 0 】

上記の課題を解決するために、請求項 3 7 に記載の発明は、記録情報を DVD 等の情報記録媒体に記録する情報記録装置に含まれるコンピュータを、予め設定された鍵情報を用いて情報記録媒体に記録すべき記録情報を暗号化し、暗号化記録情報を生成する生成手段、前記情報記録媒体に記録されている当該情報記録媒体個々に固有の識別情報を用いて前記鍵情報を暗号化し、暗号化鍵情報を生成する暗号化鍵情報生成手段、及び、前記生成された暗号化記録情報及び前記生成された暗号化鍵情報を、当該暗号化鍵情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録する記録手段、として機能させるための情報記録制御プログラムが前記コンピュータで読取可能に記録されている。

## 【 0 0 8 1 】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読

し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

#### 【0082】

上記の課題を解決するために、請求項38に記載の発明は、情報再生装置に含まれているコンピュータを、DVD等の情報記録媒体個々に固有の識別情報を用いて生成された置換情報により記録情報の一部を置換して得られる置換記録情報が記録されていると共に、当該情報記録媒体に対応する前記識別情報が記録されている情報記録媒体から前記置換記録情報を検出する検出手段、当該情報記録媒体から前記識別情報を検出する識別情報検出手段、前記検出された置換記録情報から前記置換情報を抽出する置換情報抽出手段、前記抽出された置換情報から前記識別情報を抽出する識別情報抽出手段、前記置換情報から抽出された識別情報と、前記情報記録媒体から検出された識別情報とを比較する比較手段、及び、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された置換記録情報から得られる前記記録情報の再生を行う再生手段、として機能させるための情報再生制御プログラムが前記コンピュータで読取可能に記録されている。

#### 【0083】

よって、情報記録媒体に記録されている置換記録情報が当該情報記録媒体に対応する識別情報毎に異なっていることにより当該置換記録情報が情報記録媒体個々に異なっていると共に、検出された置換記録情報と検出された識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された（すなわち、検出された識別情報と記録されている置換記録情報とが一致しない形で記録された）記録情報が再生されることを未然に防止できる。

#### 【0084】

上記の課題を解決するために、請求項39に記載の発明は、請求項38に記載の情報記録媒体において、前記置換記録情報は、予め設定された鍵情報により前

記記録情報を暗号化して得られる暗号化記録情報の一部を前記生成された置換情報により置換して得られていると共に、当該鍵情報及び前記得られた置換記録情報が前記置換情報の生成に用いられた前記識別情報に対応する前記情報記録媒体に記録されており、前記コンピュータを、当該情報記録媒体から前記鍵情報を検出する鍵情報検出手段として更に機能させると共に、前記再生手段として機能する前記コンピュータを、前記置換情報から抽出された識別情報と前記情報記録媒体から検出された識別情報とが一致したときのみ、前記検出された鍵情報を用いて前記検出された置換記録情報から得られる前記暗号化記録情報を解読し前記記録情報を再生するように機能させるための前記情報再生制御プログラムが前記コンピュータで読取可能に記録されている。

## 【 0 0 8 5 】

よって、記録情報が暗号化されて記録されていると共に、これを検出された鍵情報を用いて再生するので、不法複写された記録情報の再生を更に有効に防止できる。

## 【 0 0 8 6 】

上記の課題を解決するために、請求項 4 0 に記載の発明は、情報再生装置に含まれるコンピュータを、DVD等の情報記録媒体個々に固有の識別情報が記録されている当該情報記録媒体に記録すべき記録情報を予め設定された鍵情報を用いて暗号化して得られる暗号化記録情報と、前記識別情報を用いて前記鍵情報を暗号化して得られる暗号化鍵情報と、が記録されている前記情報記録媒体から前記暗号化記録情報及び前記暗号化鍵情報を検出する検出手段、当該情報記録媒体から前記識別情報を検出する識別情報検出手段、前記検出された暗号化鍵情報を前記検出された識別情報を用いて解読し、前記鍵情報を生成する鍵情報生成手段、及び、前記生成された鍵情報を用いて前記検出された暗号化記録情報を解読して再生する再生手段、として機能させるための情報再生制御プログラムが前記コンピュータで読取可能に記録されている。

## 【 0 0 8 7 】

よって、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されており、検出された識別情報を用いて暗号化鍵情報の暗号化を解読し当

該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生するので、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ鍵情報が取得できず、結果として記録情報の解読・再生ができないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

【 0 0 8 8 】

【発明の実施の形態】

次に本発明に好適な実施の形態について、図面に基づいて説明する。

【 0 0 8 9 】

なお、以下に説明する実施の形態は、光ディスクの一種であるDVD（従来のCD（Compact Disk）に比して約7倍以上に記録容量を高めた光ディスク）の大量生産に用いられるスタンパディスクを製造するためのカッティング装置（すなわち、再生専用のDVDの製作者が使用するカッティング装置）、記録可能なDVDに対して情報を記録するための情報記録装置及び当該DVDから情報を再生するための情報再生装置を含む不法複写防止システムに対して本発明を適用した場合の実施の形態である。

【 0 0 9 0 】

（I）不法複写防止システムの第1実施形態

始めに、本発明に係る不法複写防止システムの第1実施形態について、図1乃至図8を用いて説明する。

【 0 0 9 1 】

（A）カッティング装置の第1実施形態

始めに、不法複写防止システムの第1実施形態（以下、単に第1実施形態と称する。）に係る上記カッティング装置の実施形態について、図1乃至図5を用いて説明する。

【 0 0 9 2 】

まず、第1実施形態のカッティング装置の構成について、図1を用いて説明する。

【 0 0 9 3 】

図 1 に示すように、第 1 実施形態のカッティング装置 C 1 は、データ生成器 1 と、ECC (Error Correcting Code) エンコーダ 2 と、置換手段としての置換情報書込器 3 と、エンコーダ 4 と、レーザ発生器 5 と、記録手段としての光変調器 6 と、対物レンズ 7 と、回転サーボ回路 8 と、回転検出器 9 と、送りサーボ回路 1 0 と、位置検出器 1 1 と、送りユニット 1 2 と、スピンドルモータ 1 3 と、識別情報生成器 1 6 と、置換情報生成手段としての置換情報生成器 1 7 と、置換情報位置生成器 1 8 と、により構成されている。

## 【 0 0 9 4 】

また、スタンパディスク S P は、レジスト 1 4 と、ガラス基板 1 5 とにより構成されている。ここで、レジスト 1 4 は、後述の光ビーム B が照射されることにより感光され、当該光ビーム B の強度の変化に対応した形状の情報ピットが形成されるものである。

## 【 0 0 9 5 】

次に、概要動作を説明する。

## 【 0 0 9 6 】

先ず、データ生成器 1 は、DVD として記録すべきデータ（画像情報や音声情報又はコンピュータで活用すべきデータ等）に対して後述するデータセクタの生成処理等を施し、データ信号 S d として ECC エンコーダ 2 に出力する。

## 【 0 0 9 7 】

そして、ECC エンコーダ 2 は、データ信号 S d に含まれる記録すべきデータに対して後述する ECC ブロックの形成を施し、付加データ信号 S d e として置換情報書込器 3 に出力する。

## 【 0 0 9 8 】

次に、置換情報書込器 3 は、付加データ信号 S d e に含まれる ECC ブロックの一部を後述の置換情報 S c g に置換して置換データ信号 S d r を生成する。なお、当該置換情報 S c g としては、後述するように暗号化されたものでもよいし暗号化されていないものでもよい。

## 【 0 0 9 9 】

そして、エンコーダ 4 は、置換データ信号 S d r に含まれる ECC ブロックに対

してインターリーブ及び 8 - 1 6 変調を施し、記録データ信号  $S_r$  を生成する。

【0 1 0 0】

一方、識別情報生成器 1 6 は、記録データ信号  $S_r$  が記録される DVD（すなわち、カッティング装置 C 1 により製造されたスタンパディスク S P を用いて大量生産された DVD）一枚毎に相互に異なる識別情報  $S_{id}$  を生成し、置換情報生成器 1 7 へ出力する。

【0 1 0 1】

そして、置換情報生成器 1 7 は、当該識別情報  $S_{id}$  に対して予め設定されている暗号化処理（具体的には、ビット反転又は各ビット間のシャッフル、或いは外部要素に基づいて決定される規則に則った変形、更には後記第 2 実施形態において述べるような一方向性を有する暗号化関数を用いた変形等の暗号化処理）を施し、上記 DVD 一枚毎に異なる上記置換情報  $S_{cg}$  を生成して置換情報書込器 3 へ出力する。

【0 1 0 2】

このとき、当該置換情報  $S_{cg}$  のデータ長（ビット数）は、それを後述する ECC ブロック内に挿入した場合に、情報再生時に実行される当該 ECC ブロックに対するエラー訂正処理における訂正可能範囲内のデータ長とされている。

【0 1 0 3】

更に、置換情報位置生成器 1 8 は、当該生成された置換情報  $S_{cg}$  における各ビット毎の付加データ信号  $S_{de}$  に含まれる ECC ブロック毎への挿入位置を示す位置情報  $S_{po}$  を生成し、置換情報書込器 3 へ出力する。このとき、置換情報位置生成器 1 8 は、後述する情報再生装置 S 1 と共通化されている予め設定された挿入テーブルであって、当該 ECC ブロック毎に異なる置換情報  $S_{cg}$  の挿入位置を示す挿入テーブルに基づいて上記位置情報  $S_{po}$  を生成する。

【0 1 0 4】

これらにより、上記置換情報書込器 3 は、位置情報  $S_{po}$  により示される ECC ブロック内の挿入位置に置換情報  $S_{cg}$  における各ビットの情報を挿入して（すなわち、当該各ビットの情報により挿入位置の情報を置換して）上記置換データ信号  $S_{dr}$  を生成する。

【 0 1 0 5 】

他方、レーザ発生器 5 は、スタンパディスク S P に対して D V D としての情報ビットを形成するための光ビーム B を出射する。

【 0 1 0 6 】

そして、光変調器 6 は、レーザ発生器 5 が発生した光ビーム B を上記記録データ信号 S r を用いて強度変調する。

【 0 1 0 7 】

次に、対物レンズ 7 は、強度変調された光ビーム B をスタンパディスク S P のレジスト 1 4 上に集光する。

【 0 1 0 8 】

このとき、スピンドルモータ 1 3 はスタンパディスク S P を回転させる。

【 0 1 0 9 】

そして、回転検出器 9 はスタンパディスク S P の回転数を検出する。

【 0 1 1 0 】

これにより、回転サーボ回路 8 は、検出された回転数に基づいて、スタンパディスク S P の回転をサーボ制御する。

【 0 1 1 1 】

また、送りユニット 1 2 は、上記情報ビットが一行に並んで構成される螺旋状のトラックをスタンパディスク S P 上に形成するために、スタンパディスク S P の回転に対応してスピンドルモータ 1 3 及びスタンパディスク S P を当該スタンパディスク S P の半径方向に移動させる。

【 0 1 1 2 】

このとき、位置検出器 1 1 は送りユニット 1 2 の位置を検出する。

【 0 1 1 3 】

そして、送りサーボ回路 1 0 は検出された送りユニット 1 2 の位置に基づいて送りユニット 1 2 の移動をサーボ制御する。

【 0 1 1 4 】

以上の動作により、記録データ信号 S r に対応した情報ビットが螺旋状のトラックを形成してスタンパディスク S P のレジスト 1 4 上に形成され、 D V D 製造

のための抜き型としてのスタンパディスク S P が完成する。

【 0 1 1 5 】

この後は、当該スタンパディスク S P を用いて、樹脂成形、反射膜形成、保護層形成等のいわゆるレプリケーションプロセスが実行されて、記録データ信号 S r に対応した情報ピットを有するレプリカディスクとしての D V D が大量生産される。

【 0 1 1 6 】

なお、当該 D V D の大量生産に当たっては、上記スタンパディスク S P の製造の前後いずれかにおいて、上記置換情報 S c g に含まれている識別情報 S i d と同一の識別情報 S i d が、当該各 D V D のデータ領域以外の例えば最内周部等内に例えば当該識別情報 S i d をバーコード化する等の方法により記録される。

【 0 1 1 7 】

これにより、記録データ信号 S r として上記データ領域内に記録されている識別情報 S i d と上記最内周部等にバーコード化等されて記録されている識別情報 S i d とが一致した状態で、且つ当該識別情報 S i d が D V D 一枚毎に異なった状態で当該各 D V D が製造されることとなる。

【 0 1 1 8 】

次に、本発明に係る記録データ信号 S r 生成の細部動作について、図 1 乃至図 5 を用いて説明する。なお、図 2 は当該動作を示すフローチャートであり、図 3 乃至図 5 は当該動作により生成されるデータ（記録データ信号 S r に含まれるデータ）の構造を示す図である。

【 0 1 1 9 】

第 1 実施形態のカッティング装置 C 1 において記録データ信号 S r を生成する場合には、始めに、記録すべき元データの構造を、データセクタと称される情報単位を複数個含んだ構造に変更する。

【 0 1 2 0 】

すなわち、図 2 に示すように、先ず、記録すべき元データを 2 0 4 8 バイト毎のデータに分割し、分割した夫々のデータに対して、データセクタの開始位置を示す I D 情報と、当該 I D 情報の誤りを訂正するための I D 情報誤り訂正コード



( I E C ( I D Data Error correction Code ) ) が付加される ( ステップ S 1 ) 。

【 0 1 2 1 】

次に、ステップ S 1 で生成されたデータに対して、予備データと、分割された 2 0 4 8 バイトのデータにおけるエラーを検出するためのエラー検出コード ( E D C ( Error Detection Code ) ) が付加され、これにより、一のデータセクタが形成される ( ステップ S 2 ) 。

【 0 1 2 2 】

このデータセクタについて具体的な構成を説明すると、図 3 ( a ) に示すように、一のデータセクタ 2 0 の先頭から、 I D 情報 2 1 と、 I D 情報誤り訂正コード 2 2 と、予備データ 2 3 と、上記元データから分割されたデータ 2 4 と、エラー検出コード 2 5 とが形成される。そしてこのデータセクタ 2 0 が複数連続することにより記録すべきデータが構成される。

【 0 1 2 3 】

データセクタ 2 0 が形成されると、次に、データ 2 4 部分に対して所定のキーデータを用いてスクランブル変調が施される ( ステップ S 3 ) 。

【 0 1 2 4 】

以上説明したステップ S 1 乃至 S 3 の処理は上記データ生成器 1 において実行され、スクランブル変調されたデータ 2 4 を含む上記データ信号 S d が出力される。なお、スクランブルに用いられたキーデータは、他の画像情報等と共にデータ 2 4 として記録される。

【 0 1 2 5 】

次に、 E C C エンコーダ 2 において、データ信号 S d に含まれるデータセクタ 2 0 を用いて、 D V D に記録されたデータを再生する際に施されるエラー訂正における訂正単位である E C C ブロックが生成され、当該 E C C ブロックを含む付加データ信号 S d e が置換情報書込器 3 に出力される ( ステップ S 4 ) 。

【 0 1 2 6 】

この E C C ブロックの生成処理についてより詳細に説明すると、図 3 ( b ) に示すように、始めに、一のデータセクタ 2 0 を 1 7 2 バイト毎に分割し、分割し

た夫々のデータ（これを、以下、データブロック 3 3 という。）を垂直方向に並べる（図 3（b）左図参照）。このとき、垂直方向には 1 2 行のデータブロック 3 3 が並ぶこととなる。

#### 【0 1 2 7】

そして、垂直方向に並べた夫々のデータブロック 3 3 に対して 1 0 バイトの ECC 内符号（P I（Parity In）符号とも称され、ECC ブロック内の横一行分のデータを訂正するためのエラー訂正符号である。）3 1 を当該データブロック 3 3 の最後に付加して一の訂正ブロック 3 4 を構成する（図 3（b）右図参照）。この段階では、ECC 内符号 3 1 が付加された訂正ブロック 3 4 が垂直方向に 1 2 行並んでいることとなる。その後、この処理を 1 6 のデータセクタ 2 0 分だけ繰返す。これにより、1 9 2 行の訂正ブロック 3 4 が得られる。

#### 【0 1 2 8】

次に、上記の 1 9 2 行の訂正ブロック 3 4 が垂直方向に並べられた状態で、今度は、当該 1 9 2 行の訂正ブロック 3 4 を 1 バイト毎に最初から垂直方向に分割し、分割した夫々のデータに対して 1 6 個の ECC 外符号（P O（Parity Out）符号とも称され、ECC ブロック内の縦一列分のデータを訂正するためのエラー訂正符号である。）3 2 を付加する。なお、当該 ECC 外符号 3 2 は、上記訂正ブロック 3 4 のうち、ECC 内符号 3 1 の部分に対しても付加される。

#### 【0 1 2 9】

以上の処理により、1 6 のデータセクタ 2 0 を含む一の ECC ブロック 3 0 が図 3（b）右図に示すように形成され、当該 ECC ブロック 3 0 を含む付加データ信号 S de が置換情報書込器 3 に出力される。

#### 【0 1 3 0】

このとき、一の ECC ブロック 3 0 内に含まれる情報の総量は、

#### 【0 1 3 1】

#### 【数 1】

$(172 + 10) \text{ バイト} \times (192 + 16) \text{ 行} = 37856 \text{ バイト}$

であり、この内、実際のデータ 2 4 は、

#### 【0 1 3 2】

## 【数2】

2048バイト×16=32768バイト

となる。

## 【0133】

また、図3（b）右図に示すECCブロック30においては、1バイトのデータを「D#. \*」で示している。例えば、「D1. 0」は第1行第0列に配置されている1バイトのデータを示しており、「D190. 170」は第190行第170列に配置されている1バイトのデータを示している。従って、ECC内符号31は第172列乃至第181列に配置され、ECC外符号32は第192行乃至第207行に配置されることとなる。

## 【0134】

更に、一の訂正ブロック34はDVD上（スタンパディスクSP上）には連続して記録される。

## 【0135】

ここで、図3（b）右図に示すように、ECCブロック30をECC内符号31とECC外符号32の双方を含むように構成するのは、図3（b）右図における水平方向に並んでいるデータの訂正をECC内符号31で行い、図3（b）右図における垂直方向に並んでいるデータの訂正をECC外符号32で行うためである。

## 【0136】

すなわち、図3（b）右図で示すECCブロック30内においては、水平方向と垂直方向の二重に誤り訂正することが可能となり、従来のCD等に用いられている誤り訂正処理に比してより強力に誤り訂正ができるように構成されている。

## 【0137】

この点について更に具体的には、例えば、一の訂正ブロック34（上述のように、一行分のECC内符号31を含んで計182バイトのデータにより構成され、連続してDVD上に記録される。）が全てDVDのキズ等により破壊されたとしても、それを垂直方向から見ると、1列のECC外符号32に対して1バイトのデータ破壊でしかない。従って、夫々の列のECC外符号32を用いて誤り訂

正を行えば、たとえ一の訂正ブロック 3 4 の全てが破壊されていても、正しく誤り訂正を行って正確に再生することができるのである。

## 【 0 1 3 8 】

次に、置換情報書込器 3 において、上述のようにして生成した ECC ブロック 3 0 内における位置情報 S po により示される位置のデータを、上記置換情報 S cg により置換する（ステップ S 5）。

## 【 0 1 3 9 】

この置換処理について図 4 を用いて説明すると、上記位置情報 S po に対応する上記挿入テーブル（上記したように、後述する情報再生装置 S 1 と共有化されている。）により示される ECC ブロック 3 0 内の位置における 1 バイトのデータの一部が、置換情報 S cg の各ビットのデータである置換情報 3 5 により置換される。

## 【 0 1 4 0 】

ステップ S 5 において置換情報 3 5 が書き込まれると、当該置換情報 3 5 が含まれる ECC ブロック 3 0' により構成される上記置換データ信号 S dr がエンコーダ 4 に出力される。

## 【 0 1 4 1 】

次に、エンコーダ 4 において、置換データ信号 S dr に含まれる ECC ブロック 3 0' に対してインターリーブ及び 8 - 1 6 変調が施され、上記記録データ信号 S r が出力される（ステップ S 6 及び S 7）。

## 【 0 1 4 2 】

このステップ S 6 及び S 7 の処理について、具体的に図 5 を用いて説明する。なお、図 5 において、「D #. \*」で示されるデータは、図 3（b）右図内に記述されているデータに対応している。

## 【 0 1 4 3 】

まず、ステップ S 6 において ECC ブロック 3 0' に対してインターリーブを施す際には、始めに、図 5 最上段に示すように、ECC ブロック 3 0' が訂正ブロック 3 4 毎に水平方向に一行に並べられる。そして当該並べられたデータを一定の規約の下に並べ替えることによりインターリーブが施され、当該 ECC ブロ

ック 3 0' 分の情報が 1 6 のレコーディングセクタ 4 0 に分割される。このとき、一のレコーディングセクタ 4 0 は、2 3 6 6 バイト (3 7 8 5 6 バイト ÷ 1 6) の情報を含むこととなり、この中には、データセクタ 2 0 と ECC 内符号 3 1 または ECC 外符号 3 2 並びに識別情報 3 5 が混在している。但し、各レコーディングセクタ 4 0 の先頭には、データセクタ 2 0 における ID 情報 2 1 (図 3 (a) 参照) が配置される。

## 【0 1 4 4】

そして、一のレコーディングセクタ 4 0 は、9 1 バイト毎のデータ 4 1 に分割され、夫々にヘッダ H が付加される。その後、この状態のレコーディングセクタ 4 0 を 8 - 1 6 変調することにより、夫々のデータ 4 1 毎に一のシンクフレーム 4 2 が形成される。このとき、一のシンクフレーム 4 2 はヘッダ H' とデータ 4 3 とにより構成されている。また、一のシンクフレーム 4 2 内の情報量は、

## 【0 1 4 5】

## 【数 3】

$$91 \text{ バイト} \times 8 \times (16 / 8) = 1456 \text{ バイト}$$

となり、このシンクフレーム 4 2 が連続した形態で DVD に情報が書き込まれる。このとき、一のレコーディングセクタ 4 0 は、2 6 のシンクフレーム 4 2 を含むこととなる。

## 【0 1 4 6】

以上説明したフォーマットを構成して DVD (スタンパディスク SP) にデータが記録されることにより、当該データを再生する際に 8 - 1 6 復調及びデインターリーブを行えば (図 5 参照)、もとの ECC ブロック 3 0' を復元することができ、上記したように強力な誤り訂正を行って情報を正確に再生することができるのである。

## 【0 1 4 7】

(B) 情報記録装置の第 1 実施形態

次に、第 1 実施形態に係る上記情報記録装置の実施形態について、図 6 を用いて説明する。

## 【0 1 4 8】

なお、図6において、図1に示すカッティング装置C1と同一の動作を行う構成部材については同一の部材番号を付して細部の説明は省略する。

## 【0149】

まず、第1実施形態の情報記録装置の構成について説明する。

## 【0150】

図6に示すように、第1実施形態の情報記録装置R1は、カッティング装置C1の場合と同様のデータ生成器1、ECCエンコーダ2、置換情報書込器3、エンコーダ4、置換情報生成器17、置換情報位置生成器18と、ピックアップ50と、スピンドルモータ51と、サーボIC (Integrated Circuit) 52と、システムコントローラ53と、ストラテジ回路54と、により構成されている。

## 【0151】

また、情報記録装置R1により情報が記録されるDVD100は、いわゆるDVD-R (DVD-Recordable。一回のみ記録可能なDVD) 又はDVD-RW (DVD-Re-Recordable。複数回の記録が可能なDVD) 等の記録可能なDVDであり、夫々のDVD100には、一枚毎に異なる識別情報Sidがその最内周部等にバーコード化等されることにより予め記録されている。

## 【0152】

次に、各部の動作を説明する。

## 【0153】

先ず、データ生成器1、ECCエンコーダ2、置換情報書込器3、エンコーダ4、置換情報生成器17及び置換情報位置生成器18は、上述したカッティング装置C1の場合と同様の動作を行い、上述した形状のECCブロック30' (図4参照) を含む上記記録データ信号Srを生成してストラテジ回路54へ出力する。

## 【0154】

このとき、置換情報生成器17は、情報記録に先立ってDVD100から検出された上記識別情報Sidを用いて上述したカッティング装置C1の場合と同様の動作により上記置換情報Scgを生成する。

## 【0155】

更に、置換情報生成器 1 7 及び置換情報位置生成器 1 8 の動作は、システムコントローラ 5 3 からの制御信号 S ci 及び S cp により一元的に制御されている。

## 【 0 1 5 6 】

次に、ストラテジ回路 5 4 は、記録データ信号 S r に対して、後述するように DVD 1 0 0 上に形成される情報ピットの形状を整形するためのいわゆるストラテジ処理を施し、記録信号 S rs を生成してピックアップ 5 0 に出力する。

## 【 0 1 5 7 】

そして、ピックアップ 5 0 は、当該記録信号 S rs に基づいて記録用の光ビーム B の強度を制御し、DVD 1 0 0 上のデータ領域内に形成されている情報トラック上に上記情報ピットを形成することで、記録信号 S rs を当該 DVD 1 0 0 に記録すると共に、当該記録に先立って DVD 1 0 0 上の記録位置から上記識別情報 S id を検出して置換情報生成器 1 7 へ出力する。

## 【 0 1 5 8 】

このとき、当該 DVD 1 0 0 は、サーボ IC 5 2 からのスピンドル制御信号 S ss に基づいて回転制御されているスピンドルモータ 5 1 により予め設定された回転数で回転されている。

## 【 0 1 5 9 】

更に、当該光ビーム B の集光位置と DVD 1 0 0 上の上記情報トラックの位置との DVD 1 0 0 に水平な方向のずれ及び垂直な方向のずれは、光ビーム B を集光するためのピックアップ 5 0 内の図示しない対物レンズがサーボ IC 5 2 からのピックアップ制御信号 S sp に基づいて当該水平な方向及び垂直な方向に移動されることで解消される。

## 【 0 1 6 0 】

このため、システムコントローラ 5 3 は、上記制御信号 S ci 及び S cp に加えてサーボ IC 5 2 に上記スピンドル制御信号 S ss 及びピックアップ制御信号 S sp を出力させるための制御信号 S cs を生成して当該サーボ IC 5 2 に出力する。

## 【 0 1 6 1 】

なお、上述した情報記録装置 R 1 により DVD 1 0 0 に記録される記録データ信号 S r における上記物理的なデータ構造は、上記カッティング装置 C 1 の場合

と同様の構造を有している。

【0162】

これらの処理と並行して、上記システムコントローラ53は、上記各制御信号Sci、Scs及びScpを生成して上述した各構成部材における動作を制御すると共に、併せて情報記録装置R1全体の制御処理を行う。このとき、当該制御処理に必要な情報は図示しない操作パネルを介して外部から入力される。

【0163】

更に、情報記録装置R1の動作状態等は、必要に応じて液晶ディスプレイ等の図示しない表示部に表示される。

【0164】

以上の情報記録装置R1の動作により、DVD100の最内周部に予め記録されている上記識別情報Sid（DVD100一枚毎に異なる識別情報Sid）と同一の識別情報Sid（又は暗号化等の処理が施された識別情報Sid）が挿入された記録データ信号Srが当該DVD100におけるデータ領域内に記録されることとなる。

【0165】

（C）情報再生装置の第1実施形態

次に、上記カッティング装置C1よりデータが記録されたスタンパディスクSPを用いて製造されたDVD又は上記情報記録装置R1によりデータが記録されたDVD上の当該データを再生するための第1実施形態の情報再生装置の実施形態について、図7及び図8を用いて説明する。

【0166】

なお、以下に説明する情報再生装置は、当該DVDにデータとして画像情報及び音声情報の双方が記録されている場合に、当該画像情報及び音声情報を再生する機能を有する情報再生装置である。

【0167】

始めに、第1実施形態の情報再生装置の構成について、図7を用いて説明する。

【0168】



図 7 に示すように、第 1 実施形態の情報再生装置 S 1 は、検出手段、識別情報検出手段及び鍵情報検出手段としてのピックアップ 6 0 と、スピンドルモータ 6 1 と、R F (Radio Frequency) アンプ 6 2 と、デコーダ (復号器) 6 3 と、置換情報抽出手段としての置換情報抽出器 6 4 と、エラー訂正回路 6 5 と、再生手段としての出力制御器 6 6 と、置換情報位置生成器 6 7 と、識別情報抽出手段としての識別情報抽出器 6 8 と、比較手段としての識別情報比較器 6 9 と、システムコントローラ 7 0 と、サーボ I C 7 1 と、により構成される。

【 0 1 6 9 】

次に、動作を説明する。

【 0 1 7 0 】

上述のスタンパディスク S P を用いて製造された D V D 又は情報記録装置 R 1 により情報が記録された D V D (いずれも、上記識別情報 S i d が別個に記録されている D V D であり、以下、これらを単に D V D と称する。) 1 0 0 は、サーボ I C 7 1 からのスピンドル制御信号 S s s p に基づいて回転制御されているスピンドルモータ 6 1 により予め設定された回転数で回転されている。

【 0 1 7 1 】

そして、ピックアップ 6 0 は、回転する D V D 1 0 0 に対して情報再生用の光ビーム B を照射し、その反射光に基づいて、D V D 1 0 0 に形成されている情報ピットに対応する検出信号 S p を生成し、R F アンプ 6 2 に出力する。

【 0 1 7 2 】

なお、当該検出信号 S p には、D V D 1 0 0 の最内周部等に記録されており、当該最内周部に光ビーム B を照射して得られる上記反射光に基づいて検出された上記識別情報 S i d も含まれている。

【 0 1 7 3 】

また、当該再生用の光ビーム B の集光位置と D V D 1 0 0 上の上記情報トラックの位置との D V D 1 0 0 に水平な方向のずれ及び垂直な方向のずれは、情報記録装置 R 1 の場合と同様に、ピックアップ 6 0 内の図示しない対物レンズがサーボ I C 7 1 からのピックアップ制御信号 S s p p に基づいて当該水平な方向及び垂直な方向に移動されることで解消される。

## 【0174】

このため、システムコントローラ70は、サーボIC71に上記スピンドル制御信号Sssp及びピックアップ制御信号Ssppを出力させるための制御信号Scspを生成してサーボIC71に出力する。

## 【0175】

次に、RFアンプ62は、入力された検出信号Spに基づいて、DVD100に記録されているデータに対応するRF信号Srfを生成してデコーダ63に出力すると共に、上記検出された識別情報Sidをそのまま識別情報比較器69へ出力する。

## 【0176】

そして、デコーダ63は、当該RF信号Srfに対してデインターリーブ及び8-16復調(図5参照)を施し、上記ECCブロック30'を含む再生信号Sdcを生成して置換情報抽出器64に出力する。

## 【0177】

次に、置換情報抽出器64は、再生信号Sdc内に含まれているECCブロック30'における後述する位置情報Spoにより示される位置から、当該位置に挿入されている上記置換情報Scgを複写抽出して識別情報抽出器68へ出力すると共に、当該置換情報Scgが複写抽出された後の上記再生信号Sdcをエラー訂正回路65へ出力する。

## 【0178】

このとき、置換情報抽出器64としては、再生信号Sdcから置換情報Scgを複写抽出する他に、置換情報Scgを抽出後における当該再生信号Sdc内の当該置換情報Scgが含まれていた位置の情報を例えば全てゼロデータに置換した後にエラー訂正回路65へ出力してもよい。

## 【0179】

これと並行して、置換情報位置生成器67は、システムコントローラ70からの制御信号Scppに基づいて、上記再生信号Sdc中の各ECCブロック30'における置換情報Scgの挿入位置を示す上記位置情報Spoを、上記置換情報位置生成器18と共通化されている上記挿入テーブルを用いて当該各ECCブロック3

0' 毎に生成して置換情報抽出器 6 4 へ出力する。

【 0 1 8 0 】

これにより、識別情報抽出器 6 8 は、システムコントローラ 7 0 からの制御信号 S<sub>pu</sub>に基づいて、上述した置換情報生成器 1 7 における暗号化処理に対応する復号処理を実行し、入力されている置換情報 S<sub>cg</sub>から DVD 1 0 0 内のデータ領域内にデータとして記録されていた識別情報 S<sub>idp</sub>（すなわち、記録データ信号 S<sub>r</sub>内に挿入されていた識別情報 S<sub>id</sub>）を抽出し、識別情報比較器 6 9 へ出力する。

【 0 1 8 1 】

そして、識別情報比較器 6 9 は、R F アンプ 6 2 から出力されてきた識別情報 S<sub>id</sub>と上記識別情報 S<sub>idp</sub>とが一致した場合のみ（すなわち、記録データ信号 S<sub>r</sub>内に挿入されていた識別情報 S<sub>id</sub>と DVD 1 0 0 の最内周部等に記録されている識別情報 S<sub>id</sub>が一致した場合のみ）、出力制御器 6 6 からの後述する出力信号 S<sub>out</sub>の出力を許可する許可信号 S<sub>co</sub>を生成して当該出力制御器 6 6 へ出力する。

【 0 1 8 2 】

一方、エラー訂正回路 6 5 は、入力された再生信号 S<sub>dc</sub>内に含まれている上記 ECC ブロック 3 0'（置換情報 S<sub>cg</sub>複写抽出後の ECC ブロック 3 0'）に対して上記 ECC 内符号 3 1 及び ECC 外符号 3 2 を用いたエラー訂正処理を施し、エラー訂正信号 S<sub>cr</sub>を生成して上記出力制御器 6 6 へ出力する。

【 0 1 8 3 】

そして、出力制御器 6 6 は、上記許可信号 S<sub>co</sub>において出力信号 S<sub>out</sub>の出力が許可されている場合にのみ、上記エラー訂正信号 S<sub>cr</sub>を当該出力信号 S<sub>out</sub>として外部のディスプレイ又はスピーカ等へ出力する。

【 0 1 8 4 】

これらの処理と並行して、上記システムコントローラ 7 0 は、上記各制御信号 S<sub>csp</sub>、S<sub>pu</sub>及び S<sub>csp</sub>を生成して上述した各構成部材における動作を制御すると共に、併せて情報再生装置 S 1 全体の制御処理を行う。このとき、当該制御処理に必要な情報は図示しない操作パネルを介して外部から入力される。

【 0 1 8 5 】

更に、情報再生装置 S 1 の動作状態等は、必要に応じて液晶ディスプレイ等の図示しない表示部に表示される。

## 【 0 1 8 6 】

なお、上述した出力制御器 6 6 については、図 7 に示すようにエラー訂正回路 6 5 の後段ではなく、当該エラー訂正回路 6 5 の前段に当該出力制御器 6 6 を配置し、この段階で許可信号 S co に応じて出力信号 S out の出力制限を行うようにしてもよい。

## 【 0 1 8 7 】

次に、本発明に係る DVD 1 0 0 に記録されているデータの再生動作について、図 7 及び図 8 を用いて説明する。なお、図 8 は当該再生動作を示すフローチャートである。

## 【 0 1 8 8 】

再生動作においては、図 8 に示すように、始めに、DVD 1 0 0 に対して光ピックアップ 6 0 から情報再生用の光ビーム B を照射し、その反射光を用いて DVD 1 0 0 に記録されているデータを再生する（ステップ S 1 0）。この時には、RF アンプ 6 2 により RF 信号 S rf が生成されてデコーダ 6 3 に出力されると共に、上記識別情報 S id も併せて検出され、識別情報比較器 6 9 へ出力される。

## 【 0 1 8 9 】

次に、デコーダ 6 3 において RF 信号 S rf に対してデインターリーブ及び 8 - 1 6 復調が施され（ステップ S 1 1）、再生信号 S dc が生成される。

## 【 0 1 9 0 】

この再生信号 S dc の段階では、DVD 1 0 0 から検出されたデータは、デインターリーブ及び 8 - 1 6 復調により図 4 に示す ECC ブロック 3 0' が複数個含まれた状態となっている。

## 【 0 1 9 1 】

次に、置換情報抽出器 6 4 において、再生信号 S dc 内の ECC ブロック 3 0' のうち、上記置換情報 3 5 が記録されている領域（図 4 参照）のデータが検出され、置換情報 S cg として識別情報抽出器 6 8 に出力される（ステップ S 1 2）。

## 【 0 1 9 2 】

このとき、当該置換情報 3 5 が含まれている ECC ブロック 3 0' 内の領域の当該 ECC ブロック 3 0' 内における位置については、上記位置情報 S<sub>po</sub>により示されて置換情報抽出器 6 4 へ入力されており、この位置情報 S<sub>po</sub>の内容を参照することにより置換情報 S<sub>cg</sub>が検出される。

## 【 0 1 9 3 】

更に置換情報抽出回路 6 4 は、入力された再生信号 S<sub>dc</sub>から置換情報 S<sub>cg</sub>を複写抽出した後の情報をエラー訂正回路 6 5 に出力する。

## 【 0 1 9 4 】

そして、エラー訂正回路 6 5 は、再生信号 S<sub>dc</sub>に含まれているデータを ECC ブロック 3 0' 内の ECC 内符号 3 1 及び ECC 外符号 3 2 を用いてエラー訂正し、上記エラー訂正信号 S<sub>cr</sub>を生成して出力制御器 6 6 へ出力する。

## 【 0 1 9 5 】

なお、当該エラー訂正信号 S<sub>cr</sub>に対しては、出力制御器 6 6 へ入力されるまでにいわゆるデスクランブル処理が施されている（ステップ S 1 3）。

## 【 0 1 9 6 】

次に、識別情報比較器 6 9 において上記識別情報 S<sub>id</sub>と上記識別情報 S<sub>idp</sub>との比較処理が実行され（ステップ S 1 4）、それらが一致した場合のみ（ステップ S 1 4 ; y e s）出力制御器 6 6 からの後述する出力信号 S<sub>out</sub>の出力を許可する許可信号 S<sub>co</sub>を生成して上記出力信号 S<sub>out</sub>を外部へ出力する（ステップ S 1 5）。

## 【 0 1 9 7 】

なお、ECC ブロック 3 0' 内の置換情報 3 5 は、エラー訂正回路 6 5 におけるエラー訂正ではエラーとして扱われて訂正されるため再生され出力された出力信号 S<sub>out</sub>内からは消滅する。

## 【 0 1 9 8 】

一方、ステップ S 1 4 の判定において、二つの識別情報 S<sub>idp</sub>及び S<sub>id</sub>が一致しないときは（ステップ S 1 4 ; n o）、DVD 1 0 0 に記録されていたデータが正規に記録されたデータではなく、従って不法複写されたデータであるとして、そのままデータの出力処理を実行せずに処理を終了する。

## 【 0 1 9 9 】

なお、上記置換情報 S<sub>cg</sub>が一方向性を有する暗号化関数を用いて暗号化された識別情報 S<sub>id</sub>を含んでいる場合には、情報再生装置 S<sub>1</sub>における再生処理においては、DVD 1 0 0 から検出された識別情報 S<sub>id</sub>に対して当該暗号化関数を用いた暗号化処理を施したものと抽出された置換情報 S<sub>cg</sub>から更に抽出される上記暗号化された識別情報 S<sub>idp</sub>とを比較し、それらが一致していれば、ステップ S<sub>15</sub>等の再生処理が実行されることとなる。

## 【 0 2 0 0 】

以上説明したように、第 1 実施形態の不法複写防止システムの動作によれば、DVD 1 0 0 個々に固有の識別情報 S<sub>id</sub>を用いて生成された置換情報 S<sub>cg</sub>により付加データ信号 S<sub>de</sub>の一部を置換した記録データ信号 S<sub>r</sub>が当該置換情報 S<sub>cg</sub>の生成に用いられた識別情報 S<sub>id</sub>に対応する DVD 1 0 0 に記録されているので、当該 DVD 1 0 0 に記録される記録データ信号 S<sub>r</sub>が当該 DVD 1 0 0 に対応する識別情報 S<sub>id</sub>毎に異なることとなり、結果として記録されている記録データ信号 S<sub>r</sub>が DVD 1 0 0 個々に異なることとなる。

## 【 0 2 0 1 】

これと共に、当該記録データ信号 S<sub>r</sub>の再生時において記録データ信号 S<sub>r</sub>内の識別情報 S<sub>id</sub>とそれが記録されていた DVD 1 0 0 に対応する識別情報 S<sub>id</sub>とを比較してそれらが一致している場合にのみ再生を許可するので、不法複写された（すなわち、DVD 1 0 0 に対応する識別情報 S<sub>id</sub>と記録データ信号 S<sub>r</sub>内の識別情報 S<sub>id</sub>とが一致しない形で複写された）記録データ信号 S<sub>r</sub>が再生されることを防止できる。

## 【 0 2 0 2 】

また、置換情報 S<sub>cg</sub>が挿入される ECC ブロック 3 0 内の位置が当該 ECC ブロック 3 0 毎に変更されているので、不法複写された記録データ信号 S<sub>r</sub>の再生を更に困難にすることができる。

## 【 0 2 0 3 】

なお、上述した第 1 実施形態においては、置換情報 S<sub>cg</sub>の書込み時においては、識別情報 S<sub>id</sub>に対して予め設定された暗号化処理を施すことで当該置換情報 S

cgを生成したが、これ以外に、当該識別情報Sidに対して何ら暗号化処理を施すことなくそれをそのまま置換情報ScgとしてECCブロック30内に書き込んでよい。

【0204】

この構成によれば、情報再生時におけるその復号処理を省略して簡易に識別情報Sidが得られることとなる。

【0205】

#### (II) 不法複写防止システムの第2実施形態

始めに、本発明に係る不法複写防止システムの第2実施形態（以下、単に第2実施形態と称する。）について、図9乃至図12を用いて説明する。

【0206】

上述した第1実施形態においては、DVD100個々に固有の識別情報Sidを含む置換情報ScgによりECCブロック30に一部を置換して記録データ信号Srを生成してDVD100に記録すると共に、当該記録データ信号Srの再生時において当該記録データSr内の識別情報Sidと別途DVD100自体から検出される当該DVD100個有の識別情報Sidとを比較することにより不法複写の有無を認識したが、以下に説明する第2実施形態では、当該識別情報Sidを含む置換情報Scg自体を更に高度に暗号化すると共に、DVD100に記録すべき元のデータであるデータ信号Sd自体をも鍵情報を用いて更に高度に暗号化する。

【0207】

#### (A) カッティング装置の第2実施形態

始めに、第2実施形態に係るカッティング装置の実施形態について、図9及び図10を用いて説明する。

【0208】

なお、図9において、第1実施形態のカッティング装置C1と同様の動作をする構成部材については、同一の番号を付して細部の説明は省略する。

【0209】

図9に示すように、第2実施形態に係るカッティング装置C2は、第1実施形態に係るカッティング装置C1の場合と同様のデータ生成器1、ECCエンコー

ダ 2、置換情報書込器 3、エンコーダ 4、レーザ発生器 5、光変調器 6、対物レンズ 7、回転サーボ回路 8、回転検出器 9、送りサーボ回路 10、位置検出器 11、送りユニット 12、スピンドルモータ 13 及び識別情報生成器 16 に加えて、鍵情報暗号化手段及び識別情報暗号化手段としての置換情報生成器 75 と、生成手段としてのデータ暗号化器 76 と、置換情報位置生成器 77 と、鍵情報生成器 78 と、を備えている。

【0210】

次に、動作を説明する。

【0211】

先ず、鍵情報生成器 78 は、後述するように上記データ信号  $S_d$  をいわゆる鍵情報を用いた予め設定された暗号化方法により暗号化するための当該鍵情報  $S_k$  を生成してデータ暗号化器 76 及び置換情報生成器 75 に出力する。

【0212】

一方、識別情報生成器 16 は、第 1 実施形態の場合と同様にして識別情報  $S_{id}$  を生成し、置換情報生成器 75 及び置換情報位置生成器 77 へ出力する。

【0213】

他方、データ生成器 1 は、第 1 実施形態の場合と同様にして上記データ信号  $S_d$  を生成し、データ暗号化器 76 へ出力する。

【0214】

これらにより、データ暗号化器 76 は、上記鍵情報  $S_k$  を用いた上記暗号化方法によりデータ信号  $S_d$  に含まれるデータを暗号化し、暗号化データ信号  $S_{ad}$  を生成して ECC エンコーダ 2 に出力する。

【0215】

そして、ECC エンコーダ 2 は、暗号化データ信号  $S_{ad}$  に対して第 1 実施形態の場合と同様にして ECC ブロックの形成処理を施し、上記付加データ信号  $S_{de}$  として置換情報書込器 3 に出力する。

【0216】

次に、置換情報書込器 3 は、第 1 実施形態の場合と同様にして付加データ信号  $S_{de}$  に含まれる ECC ブロックの一部を置換情報  $S_{cg'}$  に置換して置換データ信



号 Sdr を生成する。

【 0 2 1 7 】

そして、エンコーダ 4 は、第 1 実施形態の場合と同様にして記録データ信号 S r を生成する。

【 0 2 1 8 】

一方、置換情報生成器 7 5 は、図 1 0 に示す種々の方法のうちいずれか一つの方法を用いて、識別情報生成器 1 6 からの識別情報 S id ( カッティング装置 C 2 により製造されたスタンパディスク S P を用いて大量生産される DVD 一枚毎に相互に異なる識別情報 S id ) と鍵情報生成器 7 8 からの鍵情報 S k とを重畳し、第 2 実施形態に係る置換情報 S cg' を生成して置換情報書込器 3 へ出力する。

【 0 2 1 9 】

これと並行して、置換情報位置生成器 7 7 は、当該生成された置換情報 S cg' における各ビット毎の付加データ信号 S de に含まれる ECC ブロック毎への挿入位置を示す位置情報 S po を生成し、置換情報書込器 3 へ出力する。

【 0 2 2 0 】

より具体的には、置換情報位置生成器 7 7 は、後述する情報再生装置 S 2 と共通化されている第 1 実施形態の場合と同様の複数種類の挿入テーブルのうちの何れかに基づいて上記位置情報 S po を生成するのであるが、このとき、何れの挿入テーブルを用いて位置情報 S po を生成するかについては識別情報生成器 1 6 から入力されている識別情報 S id により規定される規則性に基づいて決定される。これにより、位置情報 S po の内容は識別情報 S id 毎に異なることとなる。

【 0 2 2 1 】

これらにより、上記置換情報書込器 3 は、位置情報 S po により示される ECC ブロック内の挿入位置に置換情報 S cg' における各ビットの情報を挿入して上記置換データ信号 S dr を生成する。

【 0 2 2 2 】

その後は、レーザ発生器 5、光変調器 6、対物レンズ 7、回転サーボ回路 8、回転検出器 9、送りサーボ回路 1 0、位置検出器 1 1、送りユニット 1 2 及びスピンドルモータ 1 3 が第 1 実施形態の場合と同様に動作することにより、記録デ

ータ信号  $S_r$  に対応した情報ピットが螺旋状のトラックを形成してスタンパディスク  $SP$  のレジスト 14 上に形成され、DVD 製造のための抜き型としてのスタンパディスク  $SP$  が完成する。

#### 【0223】

この後は、当該スタンパディスク  $SP$  を用いて、樹脂成形、反射膜形成、保護層形成等のいわゆるレプリケーションプロセスが実行されて、記録データ信号  $S_r$  に対応した情報ピットを有するレプリカディスクとしての DVD が大量生産される。

#### 【0224】

なお、当該 DVD の大量生産に当たっては、第 1 実施形態の場合と同様に、上記置換情報  $S_{cg}'$  に含まれている識別情報  $S_{id}$  と同一の識別情報  $S_{id}$  が、当該各 DVD のデータ領域以外の例えば最内周部等内に例えば当該識別情報  $S_{id}$  をバーコード化する等の方法により記録される。

#### 【0225】

これにより、記録データ信号  $S_r$  として上記データ領域内に記録されている識別情報  $S_{id}$  と上記最内周部等にバーコード化等されて記録されている識別情報  $S_{id}$  とが一致した状態で、且つ当該識別情報  $S_{id}$  が DVD 一枚毎に異なった状態で当該各 DVD が製造されることとなる。

#### 【0226】

次に、上記置換情報生成器 75 における置換情報  $S_{cg}'$  の生成処理における種々の形態について、図 10 を用いて説明する。

#### 【0227】

まず、第 1 の形態としては、図 10 (a) に示すように、置換情報生成器 75 を暗号化器 95 及び加算器 96 により構成する。

#### 【0228】

そして、暗号化器 95 において識別情報  $S_{id}$  を用いて予め設定された暗号化方法により鍵情報  $S_k$  を暗号化して暗号化鍵情報  $S_{ks}$  を生成し、更に当該暗号化鍵情報  $S_{ks}$  と識別情報  $S_{id}$  とを加算器 96 により加算して上記置換情報  $S_{cg}'$  を生成するように構成することができる。

## 【 0 2 2 9 】

このとき、具体的な加算形態としては、例えば、置換情報  $S_{cg}'$  における上位 3 ビットを暗号化鍵情報  $S_{ks}$  とし、下位 3 ビットを識別情報  $S_{id}$  として合計 6 ビットで置換情報  $S_{cg}'$  を生成する方法がある。

## 【 0 2 3 0 】

また、第 2 の形態としては、図 1 0 ( b ) に示すように、置換情報生成器 7 5 を暗号化器 9 5、加算器 9 6 及び関数化器 9 7 により構成する。

## 【 0 2 3 1 】

そして、まず、関数化器 9 7 により予め設定されている一方向性を有する暗号化関数を用いて識別情報  $S_{id}$  を関数化し、関数化識別情報  $S_{fid}$  を生成して暗号化器 9 5 へ出力する。

## 【 0 2 3 2 】

このとき、上記一方向性を有する暗号化関数とは、識別情報  $S_{id}$  から関数化識別情報  $S_{fid}$  を演算することは可能であるが、当該関数化識別情報  $S_{fid}$  から元の識別情報  $S_{id}$  を求めることが困難であるか又は実質的に不可能であるか或いは全く不可能であるような関数を言い、具体的には、例えば圧縮処理を繰り返す関数や不可逆関数等が用いられる。

## 【 0 2 3 3 】

これにより、暗号化器 9 5 は関数化識別情報  $S_{fid}$  を用いて上記暗号化方法により鍵情報  $S_k$  を暗号化して暗号化鍵情報  $S_{kss}$  を生成し、更に当該暗号化鍵情報  $S_{kss}$  と識別情報  $S_{id}$  とを図 1 0 ( a ) の場合と同様に加算器 9 6 により加算して上記置換情報  $S_{cg}'$  を生成するように構成することができる。

## 【 0 2 3 4 】

更に、第 3 の形態としては、図 1 0 ( c ) に示すように、置換情報生成器 7 5 を暗号化器 9 5 及び 9 8 並びに加算器 9 6 により構成する。

## 【 0 2 3 5 】

そして、まず、暗号化器 9 8 により上記暗号化方法により識別情報  $S_{id}$  を暗号化し、暗号化識別情報  $S_{did}$  を生成して加算器 9 6 へ出力する。

## 【 0 2 3 6 】

これと並行して、暗号化器 9 5 において識別情報  $S_{id}$  を用いて上記暗号化方法により鍵情報  $S_k$  を暗号化して暗号化鍵情報  $S_{ks}$  を生成し、更に当該暗号化鍵情報  $S_{ks}$  と上記暗号化識別情報  $S_{did}$  とを図 1 0 (a) の場合と同様に加算器 9 6 により加算して上記置換情報  $S_{cg'}$  を生成するように構成することができる。

## 【 0 2 3 7 】

更にまた、第 4 の形態としては、図 1 0 (d) に示すように、置換情報生成器 7 5 を暗号化器 9 5 及び 9 8、関数化器 9 7 並びに加算器 9 6 により構成する。

## 【 0 2 3 8 】

そして、先ず、関数化器 9 7 により上記暗号化関数を用いて識別情報  $S_{id}$  を関数化し、関数化識別情報  $S_{fid}$  を生成して暗号化器 9 5 へ出力する。

## 【 0 2 3 9 】

これと並行して、暗号化器 9 8 により上記暗号化方法により識別情報  $S_{id}$  を暗号化し、暗号化識別情報  $S_{did}$  を生成して加算器 9 6 へ出力する。このとき、例えば、暗号化器 9 8 は一方向性を有する暗号化関数を用いて構成することができるが、当該暗号化関数としては、関数化器 9 7 において用いられている暗号化関数と同じものであってもよいしこれとは異なる一方向性を有する暗号化関数であってもよい。

## 【 0 2 4 0 】

そして、暗号化器 9 5 において関数化識別情報  $S_{fid}$  を用いて上記暗号化方法により鍵情報  $S_k$  を暗号化して暗号化鍵情報  $S_{kss}$  を生成し、更に当該暗号化鍵情報  $S_{kss}$  と上記暗号化識別情報  $S_{did}$  とを図 1 0 (a) の場合と同様に加算器 9 6 により加算して上記置換情報  $S_{cg'}$  を生成するように構成することができる。

## 【 0 2 4 1 】

最後に、第 5 の形態としては、図 1 0 (e) に示すように、置換情報生成器 7 5 を暗号化器 9 5、関数化器 9 7 及び加算器 9 6 により構成する。

## 【 0 2 4 2 】

そして、先ず、関数化器 9 7 により上記暗号化関数を用いて識別情報  $S_{id}$  を関数化し、関数化識別情報  $S_{fid}$  を生成して加算器 9 6 へ出力する。

## 【 0 2 4 3 】

そして、暗号化器 9 5 において識別情報  $S_{id}$  を用いて上記暗号化方法により鍵情報  $S_k$  を暗号化して暗号化鍵情報  $S_{ks}$  を生成し、更に当該暗号化鍵情報  $S_{ks}$  と上記関数化識別情報  $S_{fid}$  とを図 1 0 (a) の場合と同様に加算器 9 6 により加算して上記置換情報  $S_{cg'}$  を生成するように構成することができる。

## 【 0 2 4 4 】

なお、図 1 0 に夫々示した場合には、鍵情報  $S_k$  を暗号化器 9 5 により暗号化して置換情報  $S_{cg'}$  に含ませる構成としているが、これ以外に、当該鍵情報  $S_k$  を暗号化することなくそのままの形態で置換情報  $S_{cg'}$  に含ませるように構成することもできる。

## 【 0 2 4 5 】

また、図 1 0 に夫々示した各場合のうち、図 1 0 (b) 及び図 1 0 (d) の場合には、一方向性を有する暗号化関数により識別情報  $S_{id}$  を暗号した上で鍵情報  $S_k$  の暗号化に用いる構成としたが、これ以外に、識別情報  $S_{id}$  を、上記一方向性を有する暗号化関数を用いた暗号化処理以外の他の暗号化処理により暗号化し、当該暗号化した識別情報により鍵情報  $S_k$  を暗号化するように構成することもできる。

## 【 0 2 4 6 】

更に、上述したカッティング装置 C 2 の場合には鍵情報  $S_k$  (又は暗号化した暗号鍵情報  $S_{ks}$  等) を置換情報  $S_{cg'}$  内に含ませる構成としたが、これ以外に、当該置換情報  $S_{cg'}$  内に含ませるのではなく、予め設定されている DVD 1 0 0 の最内周部に記録するように構成することもできる。

## 【 0 2 4 7 】

(B) 情報記録装置の第 2 実施形態

次に、第 2 実施形態に係る上記情報記録装置の実施形態について、図 1 1 を用いて説明する。

## 【 0 2 4 8 】

なお、図 1 1 において、図 9 に示すカッティング装置 C 2 と同一の動作を行う構成部材又は第 1 実施形態の情報記録装置 R 1 と同一の動作を行う構成部材については同一の部材番号を付して細部の説明は省略する。

## 【 0 2 4 9 】

まず、第 2 実施形態の情報記録装置の構成について説明する。

## 【 0 2 5 0 】

図 1 1 に示すように、第 2 実施形態の情報記録装置 R 2 は、カッティング装置 C 2 の場合と同様のデータ生成器 1、E C C エンコーダ 2、置換情報書込器 3、エンコーダ 4、鍵情報生成器 7 8、置換情報生成器 7 5 及び置換情報位置生成器 7 7 と、情報記録装置 R 1 の場合と同様のピックアップ 5 0、スピンドルモータ 5 1、サーボ I C 5 2、システムコントローラ 5 3 及びストラテジ回路 5 4 と、により構成されている。

## 【 0 2 5 1 】

また、情報記録装置 R 2 により情報が記録される D V D 1 0 0 は、第 1 実施形態の場合と同様に D V D - R 又は D V D - R W 等の記録可能な D V D であり、夫々の D V D 1 0 0 には、一枚毎に異なる識別情報 S i d がその最内周部等にバーコード化等されることにより予め記録されている。

## 【 0 2 5 2 】

次に、各部の動作を説明する。

## 【 0 2 5 3 】

先ず、データ生成器 1、E C C エンコーダ 2、置換情報書込器 3、エンコーダ 4、置換情報生成器 7 5 及び置換情報位置生成器 7 7 は、上述したカッティング装置 C 2 の場合と同様の動作を行い、上述した形状の E C C ブロック 3 0'（図 4 参照）を含む上記記録データ信号 S r を生成してストラテジ回路 5 4 へ出力する。

## 【 0 2 5 4 】

このとき、置換情報生成器 7 5 は、図 1 0 に示した各形態の何れか一の方法により、情報記録に先立って D V D 1 0 0 からピックアップ 5 0 を介して検出された上記識別情報 S i d 及び鍵情報 S k を用いて上記置換情報 S c g' を生成する。

## 【 0 2 5 5 】

更に、置換情報生成器 7 5 及び置換情報位置生成器 7 7 の動作は、システムコントローラ 5 3 からの制御信号 S c i 及び S c p により第 1 実施形態の場合と同様に

一元的に制御されている。

【 0 2 5 6 】

その後は、ストラテジ回路 5 4、ピックアップ 5 0、スピンドルモータ 5 1 及びサーボ I C 5 2 並びにシステムコントローラ 5 3 の第 1 実施形態の場合と同様の動作により、各サーボ制御が実行されつつ記録信号 S r s が回転する当該 D V D 1 0 0 に記録される。

【 0 2 5 7 】

以上の情報記録装置 R 2 の動作により、D V D 1 0 0 の最内周部に予め記録されている上記識別情報 S i d ( D V D 1 0 0 一枚毎に異なる識別情報 S i d ) と同一の識別情報 S i d 及び鍵情報 S k ( 或いは暗号化識別情報 S f i d 又は S d i d 及び暗号化鍵情報 S k s 又は S k s s ) が挿入されて暗号化された記録データ信号 S r が当該 D V D 1 0 0 におけるデータ領域内に記録されることとなる。

【 0 2 5 8 】

( C ) 情報再生装置の第 2 実施形態

次に、上記カッティング装置 C 2 よりデータが記録されたスタンパディスク S P を用いて製造された D V D 又は上記情報記録装置 R 2 によりデータが記録された D V D 1 0 0 上の当該データを再生するための第 2 実施形態の情報再生装置について、図 1 2 を用いて説明する。

【 0 2 5 9 】

なお、図 1 2 に示す第 2 実施形態の情報再生装置において、第 1 実施形態に係る情報再生装置 S 1 と同様の動作を行う構成部材については、同一の部材番号を付して細部の説明を省略する。

【 0 2 6 0 】

始めに、第 2 実施形態の情報再生装置の構成について、図 1 2 を用いて説明する。

【 0 2 6 1 】

図 1 2 に示すように、第 2 実施形態の情報再生装置 S 2 は、第 1 実施形態の場合と同様のピックアップ 6 0、スピンドルモータ 6 1、R F アンプ 6 2、デコーダ 6 3、置換情報抽出器 6 4、訂正手段としてのエラー訂正回路 6 5、識別情報

比較器 6 9、システムコントローラ 7 0 及びサーボ I C 7 1 と、再生手段としてのデータ復号器 8 0 と、置換情報位置生成器 8 1 と、鍵情報抽出手段、鍵情報生成手段、識別情報生成手段、暗号化識別情報抽出手段及び暗号化識別情報生成手段としての置換情報復号器 8 2 と、により構成されている。

## 【 0 2 6 2 】

次に、動作を説明する。

## 【 0 2 6 3 】

先ず、第 1 実施形態の場合と同様の動作により、回転する DVD 1 0 0 に対して各サーボ制御が実行されつつ情報再生用の光ビーム B が照射され、その反射光に基づいて DVD 1 0 0 に形成されている情報ピットに対応する検出信号 S p が生成され、R F アンプ 5 2 に出力する。

## 【 0 2 6 4 】

なお、当該検出信号 S p には、上記反射光に基づいて検出された上記識別情報 S i d も含まれている。

## 【 0 2 6 5 】

次に、R F アンプ 6 2 は、第 1 実施形態の場合と同様に R F 信号 S r f を生成してデコーダ 6 3 に出力すると共に、上記検出された識別情報 S i d をそのまま識別情報比較器 6 9、置換情報位置生成器 8 1 及び置換情報復号器 8 2 へ夫々出力する。

## 【 0 2 6 6 】

そして、デコーダ 6 3 は、当該 R F 信号 S r f に対してデインターリーブ及び 8 - 1 6 復調を施し、上記 E C C ブロック 3 0' を含む再生信号 S d c を生成して置換情報抽出器 6 4 に出力する。

## 【 0 2 6 7 】

次に、置換情報抽出器 6 4 は、再生信号 S d c 内に含まれている E C C ブロック 3 0' における後述する位置情報 S p o により示される位置から、当該位置に挿入されている上記置換情報 S c g' を複写抽出して置換情報復号器 8 2 へ出力すると共に、当該置換情報 S c g' が複写抽出された後の上記再生信号 S d c をエラー訂正回路 6 5 へ出力する。



## 【 0 2 6 8 】

このとき、置換情報位置生成器 8 1 は、システムコントローラ 7 0 からの制御信号 S c p p 及び識別情報 S i d に基づいて、上記したカッティング装置 C 2 又は情報記録装置 R 2 における置換情報位置生成器 7 7 と共通化されている挿入テーブルのうち識別情報 S i d により規定される規則性に基づいて選択された一の挿入テーブルを用いて当該置換情報位置生成器 7 7 と同様の処理を行い、識別情報 S i d 毎に異なる位置情報 S p o を各 E C C ブロック 3 0' 毎に生成して置換情報抽出器 6 4 へ出力する。

## 【 0 2 6 9 】

これにより、置換情報復号器 8 2 は、識別情報 S i d を用いて置換情報 S c g' に対してカッティング装置 C 2 又は情報記録装置 R 2 における置換情報生成器 7 5 と逆の復号処理を施し、当該置換情報 S c g' から元の鍵情報 S k 及び第 1 実施形態の場合と同様の識別情報 S i d p を生成し、当該鍵情報 S k をデータ復号器 8 0 へ出力すると共に識別情報 S i d p を識別情報比較器 6 9 へ出力する。

## 【 0 2 7 0 】

ここで、当該置換情報復号器 8 2 における復号処理は、図 1 0 に示した置換情報生成器 7 5 の各形態により異なってくる。

## 【 0 2 7 1 】

すなわち、図 1 0 ( a ) に示す第 1 の形態により置換情報生成器 7 5 が形成されていた場合には、置換情報復号器 8 2 においては、先ず、置換情報 S c g' における上下 3 ビットづつを分離することにより識別情報 S i d p 及び暗号化鍵情報 S k s を夫々生成する。

## 【 0 2 7 2 】

そして、識別情報 S i d p はそのまま識別情報比較器 6 9 へ出力すると共に、暗号化鍵情報 S k s に対して D V D 1 0 0 の最内周部に記録されていた識別情報 S i d を用いた上記暗号化器 9 5 における暗号化方法に対応する復号方法を用いた処理を施し、上記鍵情報 S k を生成してデータ復号器 8 0 へ出力する。

## 【 0 2 7 3 】

なお、このとき、暗号化鍵情報 S k s の復号化に当たり上記識別情報 S i d p を用

いて復号してもよい。

【0274】

一方、図10(b)に示す第2の形態により置換情報生成器75が形成されていた場合には、置換情報復号器82は上記関数化器97を備えることとなる。

【0275】

そして、まず、置換情報 $S_{cg'}$ における上下3ビットづつを分離することにより識別情報 $S_{idp}$ 及び暗号化鍵情報 $S_{kss}$ を夫々生成する。

【0276】

その後、識別情報 $S_{idp}$ をそのまま識別情報比較器69へ出力すると共に、DVD100の最内周部に記録されていた識別情報 $S_{id}$ を関数化器97により関数化して関数化識別情報 $S_{fid}$ を生成する。

【0277】

そして、分離した暗号化鍵情報 $S_{kss}$ に対して、上記関数化識別情報 $S_{fid}$ を用いた暗号化器95における暗号化方法に対応する復号方法を用いた処理を施し、上記鍵情報 $S_k$ を生成してデータ復号器80へ出力する。

【0278】

なお、このとき、暗号化鍵情報 $S_{kss}$ の復号化に当たり上記識別情報 $S_{idp}$ を関数化器97により関数化して得られた関数化識別情報を用いて復号してもよい。

【0279】

次に、図10(c)に示す第3の形態により置換情報生成器75が形成されていた場合には、まず、置換情報 $S_{cg'}$ における上下3ビットづつを分離することにより上記暗号化識別情報 $S_{did}$ 及び暗号化鍵情報 $S_{ks}$ を夫々生成する。

【0280】

その後、暗号化識別情報 $S_{did}$ に対してDVD100の最内周部に記録されていた識別情報 $S_{id}$ を用いた上記暗号化器98における暗号化方法に対応する復号方法を用いた処理を施し、上記識別情報 $S_{idp}$ を生成して識別情報比較器69へ出力する。

【0281】

更に、暗号化鍵情報 $S_{ks}$ に対しては上記識別情報 $S_{id}$ を用いた上記暗号化器9

5における暗号化方法に対応する復号方法を用いた処理を施し、上記鍵情報Skを生成してデータ復号器80へ出力する。

## 【0282】

なお、このとき、暗号化鍵情報Sksの復号化に当たり上記識別情報Sidpを用いて復号してもよい。

## 【0283】

他方、図10(d)に示す第4の形態により置換情報生成器75が形成されていた場合には、置換情報復号器82は上記関数化器97を備えることとなる。

## 【0284】

そして、まず、置換情報Scg'における上下3ビットづつを分離することにより暗号化識別情報Sdid及び暗号化鍵情報Skssを夫々生成する。

## 【0285】

その後、暗号化識別情報Sdidに対してDVD100の最内周部に記録されていた識別情報Sidを用いた上記暗号化器98における暗号化方法に対応する復号方法を用いた処理を施し、上記識別情報Sidpを生成して識別情報比較器69へ出力する。

## 【0286】

その後、当該識別情報Sidを関数化器97により関数化して関数化識別情報Sfidを生成する。

## 【0287】

そして、分離した暗号化鍵情報Skssに対して、上記関数化識別情報Sfidを用いた暗号化器95における暗号化方法に対応する復号方法を用いた処理を施し、上記鍵情報Skを生成してデータ復号器80へ出力する。

## 【0288】

なお、このとき、暗号化鍵情報Skssの復号化に当たり上記識別情報Sidpを関数化器97により関数化して得られた関数化識別情報を用いて復号してもよい。

## 【0289】

最後に、図10(e)に示す第5の形態により置換情報生成器75が形成されていた場合には、まず、置換情報Scg'における上下3ビットづつを分離するこ

とにより関数化識別情報  $S_{fid}$  及び暗号化鍵情報  $S_{ks}$  を夫々生成する。

【0290】

このとき、分離した関数化識別情報  $S_{fid}$  は上述したように一方向性を有する暗号化関数を用いて暗号化されているので、当該関数化識別情報  $S_{fid}$  からは最早元の識別情報  $S_{id}$  を復元することはできない。

【0291】

よって、当該分離された他方の暗号化鍵情報  $S_{ks}$  については、DVD100の最内周部に記録されていた識別情報  $S_{id}$  を用いた上記暗号化器95における暗号化方法に対応する復号方法を用いた処理を施し、上記鍵情報  $S_{k}$  を生成してデータ復号器80へ出力する。

【0292】

なお、上述したように鍵情報  $S_{k}$  を暗号化することなくそのままの形態で置換情報  $S_{cg'}$  に含ませるようにした場合については、置換情報  $S_{cg'}$  から分離された鍵情報  $S_{k}$  をそのままデータ復号器80へ出力する構成とすればよいこととなる。

【0293】

次に、識別情報比較器69は、RFアンプ62から出力されてきた識別情報  $S_{id}$  と上述した夫々の形態で生成された識別情報  $S_{idp}$  とが一致した場合のみ（すなわち、記録データ信号  $S_r$  内に挿入されていた識別情報  $S_{id}$  とDVD100の最内周部等に記録されている識別情報  $S_{id}$  が一致した場合のみ）、データ復号器80からの出力信号  $S_{out}$  の出力を許可する許可信号  $S_{co}$  を生成して当該データ復号器80へ出力する。

【0294】

このとき、図10（e）に示す第5の形態により置換情報生成器75が形成されていた場合には、上述したように分離された関数化識別情報  $S_{fid}$  からは最早元の識別情報  $S_{id}$  を復元することはできないので、このときには、DVD100の最内周部から検出された識別情報  $S_{id}$  に対して関数化識別情報  $S_{fid}$  の生成の際と同様の暗号化関数による暗号化処理を施し、その結果と上記関数化識別情報  $S_{fid}$  とを比較し、それらが一致すればデータ復号器80からの出力信号  $S_{out}$  の

出力を許可する許可信号  $S_{co}$  を生成して出力することとなる。

【 0 2 9 5 】

一方、エラー訂正回路 6 5 は、入力された再生信号  $S_{dc}$  内に含まれている上記 ECC ブロック 3 0'（置換情報  $S_{cg}$  抽出後の ECC ブロック 3 0'）に対して上記 ECC 内符号 3 1 及び ECC 外符号 3 2 を用いたエラー訂正処理を施し、エラー訂正信号  $S_{cr}$  を生成して上記データ復号器 8 0 へ出力する。

【 0 2 9 6 】

そして、データ復号器 8 0 は、上記許可信号  $S_{co}$  において出力信号  $S_{out}$  の出力が許可されている場合にのみ、上述の各形態により生成された鍵情報  $S_k$  を用いてカッティング装置 C 2 又は情報記録装置 R 2 におけるデータ暗号化器 7 6 に対応する復号処理を上記エラー訂正信号  $S_{cr}$  に対して実行し、上記出力信号  $S_{out}$  として外部のディスプレイ又はスピーカ等へ出力する。

【 0 2 9 7 】

これらの処理と並行して、上記システムコントローラ 7 0 は、上記各制御信号  $S_{cpp}$ 、 $S_u$  及び  $S_{sp}$  を生成して上述した各構成部材における動作を制御すると共に、併せて情報再生装置 S 1 全体の制御処理を行う。

【 0 2 9 8 】

なお、上述したデータ復号器 8 0 については、第 1 実施形態における出力制御器 6 6 の場合と同様に、図 1 2 に示すエラー訂正回路 6 5 の後段ではなく、当該エラー訂正回路 6 5 の前段に配置し、この段階で許可信号  $S_{co}$  に応じて出力信号  $S_{out}$  の出力制限を行うようにしてもよい。

【 0 2 9 9 】

以上説明したように、第 2 実施形態の不法複写防止システムの動作によれば、第 1 実施形態の不法複写防止システムの効果に加えて、置換情報  $S_{cg}'$  の生成に当たって種々の暗号化処理又は関数化処理を施して生成すると共に（図 1 0 参照）、これに対応して情報再生時に置換情報  $S_{cg}'$  を復号するので、上記鍵情報  $S_k$  及び識別情報  $S_{idp}$  の不法な取得を困難としてより効果的に不法な複写記録を防止することができる。

【 0 3 0 0 】

なお、上述した第2実施形態においては、鍵情報  $S_k$  を暗号化した暗号化鍵情報  $S_{ks}$  及び識別情報  $S_{id}$  を暗号化した暗号化識別情報  $S_{did}$  等により置換情報  $S_{cg'}$  を構成する場合について説明したが、これ以外に、当該暗号化鍵情報  $S_{ks}$  のみにより置換情報を生成して書き込むようにしてもよい。

#### 【0301】

この場合には、当該置換情報が、暗号化鍵情報  $S_{ks}$  の生成に用いられた識別情報  $S_{id}$  に対応する DVD 100 に記録されるので、暗号化鍵情報  $S_{ks}$  が DVD 100 個々に異なる形態で当該 DVD 100 に記録されることとなり、更に当該識別情報  $S_{id}$  を用いて暗号化鍵情報  $S_k$  の暗号化を解読し当該解読された鍵情報  $S_k$  を用いてエラー訂正信号  $S_{cr}$  の暗号化を解読して再生するように構成することで、当該識別情報  $S_{id}$  と暗号化鍵情報  $S_k$  とが正規に対応付けられなければ暗号化の復号ができないこととなるので、不法複写された（すなわち、識別情報  $S_{id}$  と暗号化鍵情報  $S_k$  とが正規に対応付けられない形で複写された）記録データ信号  $S_r$  が再生されることを防止できる。

#### 【0302】

なお、上述した各実施形態においては、DVD 100 一枚毎に異なる識別情報  $S_{id}$  を記録しておくように構成したが、特にスタンパディスク SP を用いて再生専用の DVD 100 を大量生産する場合には、例えば、同じ内容の記録データ  $S_d$  が記録される当該 DVD 100 においては全て同じ識別情報  $S_{id}$  を記録しておくように構成しても、上述した各実施形態とほぼ同様の効果が得られる。

#### 【0303】

また、上記した同一内容の記録データ  $S_d$  が記録される DVD 100 の間においても、例えば、同じロット番号を有する DVD 100 内でのみ同じ識別情報  $S_{id}$  を有するように構成することもできる。

#### 【0304】

更に、上述した各実施形態においては、DVD 100 自体に対応する識別情報  $S_{id}$  の記録位置を、当該 DVD 100 におけるデータ領域以外の最内周部である場合について説明したが、これ以外に、当該識別情報  $S_{id}$  自体を、置換情報  $S_{cg}$  又は  $S_{cg'}$  とは別個に予め設定された当該データ領域内の位置に記録するように

構成することもできる。

【0305】

この場合には、記録データ信号  $S_r$  の記録と並行して識別情報  $S_{id}$  自体の記録も実行することができるので、上述したカッティング処理及び情報記録処理を簡易化することができる。

【0306】

更に、上述した各実施形態における置換情報  $S_{cg}$  又は  $S_{cg}'$  を挿入する DVD 100 上の位置としては、上述したデータ領域以外に、例えばリードインエリア等を含む記録可能な領域内であればいずれの領域であってもよい。

【0307】

但し、この場合には、記録された記録情報の再生時に当該再生が中止される場合があることを考慮すると、再生開始当初に読み出されるべき上記リードインエリア内又はデータ領域内における管理情報が記録されている領域内に記録することが望ましい。

【0308】

更にまた、上述した各実施形態における記録処理又は再生処理に対応するプログラムをフレキシブルディスク又はハードディスク等の情報記録媒体に予め記録しておき、これをパーソナルコンピュータ等により読み出して実行することにより、当該記録処理又は再生処理を当該パーソナルコンピュータ等を中心として構成される情報記録再生システムにおいて実行するように構成することも可能である。

【0309】

また、上述した各実施形態は、記録可能な DVD 等に対して本発明を適用した場合について説明したが、これ以外に、記録可能な CD 等他の情報記録媒体に対しても本発明を適用して不法複写された記録情報が再生されることを防止することができる。

【0310】

【発明の効果】

以上説明したように、請求項 1 に記載の発明によれば、情報記録媒体に記録さ

れる置換記録情報が当該情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録されている置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらに対応関係を有している場合にのみ再生を許可することで、不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 1 1 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 1 2 】

請求項 2 に記載の発明によれば、請求項 1 に記載の発明の効果に加えて、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に有効に防止できる。

## 【 0 3 1 3 】

請求項 3 に記載の発明によれば、請求項 2 に記載の発明の効果に加えて、鍵情報を含んで置換情報が生成されているので、再生時における鍵情報の取得がより困難となり、不法複写された記録情報の再生を更に困難とすることができる。

## 【 0 3 1 4 】

請求項 4 に記載の発明によれば、請求項 2 又は 3 に記載の発明の効果に加えて、鍵情報に代えて暗号化鍵情報を記録するので、再生時における不法な鍵情報の取得及びそれを用いた記録情報の復号を防止できる。

## 【 0 3 1 5 】

請求項 5 に記載の発明によれば、請求項 4 に記載の発明の効果に加えて、生成された暗号化識別情報を用いて鍵情報を暗号化して暗号化鍵情報を生成するので、記録情報を復号するための鍵情報が当該再生時において不法に取得されることを困難とすることができる。



## 【 0 3 1 6 】

請求項 6 に記載の発明によれば、請求項 1 から 5 のいずれか一項に記載の発明の効果に加えて、識別情報に対して暗号化処理を施して得られる暗号化識別情報を用いて置換情報を生成するので、置換記録情報との比較対象となる識別情報が再生時において不法に取得されることを困難とすることができる。

## 【 0 3 1 7 】

請求項 7 に記載の発明によれば、請求項 5 又は 6 に記載の発明の効果に加えて、暗号化処理が一方向性を有する暗号化関数を用いた暗号化処理であるので、再生時における識別情報の取得を更に困難とすることができる。

## 【 0 3 1 8 】

請求項 8 に記載の発明によれば、請求項 1 から 7 のいずれか一項に記載の発明の効果に加えて、エラー訂正用の訂正符号が付加された付加記録情報の一部を置換情報に置換して置換記録情報を生成するので、再生時において正確に記録情報を再生することができる。

## 【 0 3 1 9 】

請求項 9 に記載の発明によれば、請求項 1 から 8 のいずれか一項に記載の発明の効果に加えて、置換記録情報と共に記録された識別情報と当該置換記録情報の内容とをその再生時に比較することで、正規に記録された置換記録情報のみを再生可能とすることができる。

## 【 0 3 2 0 】

請求項 1 0 に記載の発明によれば、請求項 1 から 8 のいずれか一項に記載の発明の効果に加えて、予め記録されている識別情報と当該置換記録情報の内容とをその再生時に比較することで、正規に記録された置換記録情報のみを再生可能とすることができる。

## 【 0 3 2 1 】

請求項 1 1 に記載の発明によれば、請求項 1 から 1 0 のいずれか一項に記載の発明の効果に加えて、置換情報を用いた置換態様が識別情報により変更されているので、不法複写された記録情報の再生を更に困難にすることができる。

## 【 0 3 2 2 】

請求項 1 2 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 2 3 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないので、暗号化記録情報の解読のための鍵情報が取得できないこととなり、不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 2 4 】

請求項 1 3 に記載の発明によれば、請求項 1 2 に記載の発明の効果に加えて、暗号化記録情報の一部が暗号化鍵情報とされるので、再生時における当該暗号化鍵情報の取得を困難とすることができる。

## 【 0 3 2 5 】

請求項 1 4 に記載の発明によれば、記録される置換記録情報が情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録される置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらに対応関係を有している場合にのみ再生を許可することで、情報記録媒体に不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 2 6 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再

生されることを防止することができる。

【 0 3 2 7 】

請求項 1 5 に記載の発明によれば、請求項 1 4 に記載の発明の効果に加えて、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に防止できる。

【 0 3 2 8 】

請求項 1 6 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

【 0 3 2 9 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないので、暗号化記録情報の解読のための鍵情報が取得できないこととなり、不法複写された記録情報が再生されることを防止することができる。

【 0 3 3 0 】

請求項 1 7 に記載の発明によれば、情報記録媒体に記録されている置換記録情報が当該情報記録媒体に対応する識別情報毎に異なっていることにより当該置換記録情報が情報記録媒体個々に異なっていると共に、検出された置換記録情報と検出された識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された（すなわち、検出された識別情報と記録されている置換記録情報とが一致しない形で記録された）記録情報が再生されることを未然に防止できる。

【 0 3 3 1 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、当該他の情報記録媒体から

の記録情報再生時において識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 3 2 】

請求項 1 8 に記載の発明によれば、請求項 1 7 に記載の発明の効果に加えて、記録情報が暗号化されて記録されていると共に、これを検出された鍵情報を用いて再生するので、不法複写された記録情報の再生を更に有効に防止できる。

## 【 0 3 3 3 】

請求項 1 9 に記載の発明によれば、請求項 1 8 に記載の発明の効果に加えて、再生時における鍵情報の取得がより困難となり、不法複写された暗号化記録情報の解読・再生を更に困難とすることができる。

## 【 0 3 3 4 】

請求項 2 0 に記載の発明によれば、請求項 1 8 又は 1 9 に記載の発明の効果に加えて、暗号化鍵情報が鍵情報に代えて記録されているので、記録情報の暗号化の解読に用いられる鍵情報の取得及びそれを用いた記録情報の復号を防止できる。

## 【 0 3 3 5 】

請求項 2 1 に記載の発明によれば、請求項 2 0 に記載の発明の効果に加えて、識別情報を暗号化して得られる暗号化識別情報を用いて鍵情報を暗号化して得られた暗号化鍵情報が記録されているので、記録情報を復号するための鍵情報が当該再生時において不法に取得されることを更に困難とすることができる。

## 【 0 3 3 6 】

請求項 2 2 に記載の発明によれば、請求項 2 1 に記載の発明の効果に加えて、暗号化処理が一方向性を有する暗号化関数を用いて暗号化する暗号化処理であるので、暗号化鍵情報を解読するための暗号化識別情報の不法取得を更に困難とすることができる。

## 【 0 3 3 7 】

請求項 2 3 に記載の発明によれば、請求項 1 7 から 2 2 のいずれか一項に記載の発明の効果に加えて、識別情報に対して暗号化処理を施して得られる暗号化識

別情報を用いて置換情報が生成されているので、情報記録媒体から検出された識別情報との比較対象となる識別情報を不法取得を更に困難とすることができる。

## 【 0 3 3 8 】

請求項 2 4 に記載の発明によれば、請求項 1 7 から 2 2 のいずれか一項に記載の発明の効果に加えて、抽出された暗号化識別情報と生成された副暗号化識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された記録情報が再生されることを未然に防止できる。

## 【 0 3 3 9 】

請求項 2 5 に記載の発明によれば、請求項 1 7 から 2 4 のいずれか一項に記載の発明の効果に加えて、記録情報に対して訂正符号を付加して生成される付加記録情報の一部が置換情報に置換されて置換記録情報とされているので、正確にエラー訂正を行って記録情報を再生することができる。

## 【 0 3 4 0 】

請求項 2 6 に記載の発明によれば、請求項 1 7 から 2 5 のいずれか一項に記載の発明の効果に加えて、置換態様が識別情報毎に異なることとなっており、これを検出された識別情報により特定して再生するので、不法複写された記録情報の再生を更に困難にすることができる。

## 【 0 3 4 1 】

請求項 2 7 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されており、検出された識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生するので、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ鍵情報が取得できず、結果として記録情報の解読・再生ができないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 4 2 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないので、暗号化記録情報の解読のための鍵情報が取得

できないこととなり、不法複写された記録情報が再生されることを防止することができる。

【 0 3 4 3 】

請求項 2 8 に記載の発明によれば、請求項 2 7 に記載の発明の効果に加えて、暗号化鍵情報の取得をより困難として、不法複写された暗号化記録情報の解読・再生を防止することができる。

【 0 3 4 4 】

請求項 2 9 に記載の発明によれば、情報記録媒体に記録される置換記録情報が当該情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録されている置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらが対応関係を有している場合にのみ再生を許可することで、不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

【 0 3 4 5 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再生されることを防止することができる。

【 0 3 4 6 】

請求項 3 0 に記載の発明によれば、請求項 2 9 に記載の発明の効果に加えて、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に防止できる。

【 0 3 4 7 】

請求項 3 1 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（す

なわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 4 8 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないのので、暗号化記録情報の解読のための鍵情報が取得できないこととなり、不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 4 9 】

請求項 3 2 に記載の発明によれば、情報記録媒体に記録されている置換記録情報が当該情報記録媒体に対応する識別情報毎に異なっていることにより当該置換記録情報が情報記録媒体個々に異なっていると共に、検出された置換記録情報と検出された識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された（すなわち、検出された識別情報と記録されている置換記録情報とが一致しない形で記録された）記録情報が再生されることを未然に防止できる。

## 【 0 3 5 0 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、当該他の情報記録媒体からの記録情報再生時において識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 5 1 】

請求項 3 3 に記載の発明によれば、請求項 3 2 に記載の発明の効果に加えて、記録情報が暗号化されて記録されていると共に、これを検出された鍵情報を用いて再生するので、不法複写された記録情報の再生を更に有効に防止できる。

## 【 0 3 5 2 】

請求項 3 4 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されており、検出された識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化

を解読して再生するので、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ鍵情報が取得できず、結果として記録情報の解読・再生ができないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 5 3 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のまま他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないので、暗号化記録情報の解読のための鍵情報が取得できないこととなり、不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 5 4 】

請求項 3 5 に記載の発明によれば、情報記録媒体に記録される置換記録情報が当該情報記録媒体に対応する識別情報毎に異なることとなり、結果として記録されている置換記録情報が情報記録媒体個々に異なることとなるので、当該置換記録情報の再生時において置換記録情報とそれが記録されていた情報記録媒体に対応する識別情報とを比較してそれらが対応関係を有している場合にのみ再生を許可することで、不法複写された（すなわち、識別情報と置換記録情報とが正規の対応関係を有さない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 5 5 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のまま他の情報記録媒体に不法複写されている場合でも、識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 5 6 】

請求項 3 6 に記載の発明によれば、請求項 3 5 に記載の発明の効果に加えて、記録情報が暗号化されていることにより、不法複写された記録情報の再生を更に防止できる。

## 【 0 3 5 7 】

請求項 3 7 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる



形態で当該情報記録媒体に記録されることとなるので、当該識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生することで、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ記録情報が解読・再生できないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 5 8 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないので、暗号化記録情報の解読のための鍵情報が取得できないこととなり、不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 5 9 】

請求項 3 8 に記載の発明によれば、情報記録媒体に記録されている置換記録情報が当該情報記録媒体に対応する識別情報毎に異なっていることにより当該置換記録情報が情報記録媒体個々に異なっていると共に、検出された置換記録情報と検出された識別情報とが一致したときのみ記録情報の再生が行われるので、不法複写された（すなわち、検出された識別情報と記録されている置換記録情報とが一致しない形で記録された）記録情報が再生されることを未然に防止できる。

## 【 0 3 6 0 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、当該他の情報記録媒体からの記録情報再生時において識別情報と置換記録情報とが正規の対応関係を有さないこととなるので、当該不法複写された記録情報が再生されることを防止することができる。

## 【 0 3 6 1 】

請求項 3 9 に記載の発明によれば、請求項 3 8 に記載の発明の効果に加えて、記録情報が暗号化されて記録されていると共に、これを検出された鍵情報を用いて再生するので、不法複写された記録情報の再生を更に有効に防止できる。

## 【 0 3 6 2 】

請求項 4 0 に記載の発明によれば、暗号化鍵情報が情報記録媒体個々に異なる形態で当該情報記録媒体に記録されており、検出された識別情報を用いて暗号化鍵情報の暗号化を解読し当該解読された鍵情報を用いて暗号化記録情報の暗号化を解読して再生するので、当該識別情報と暗号化鍵情報とが正規に対応付けられなければ鍵情報が取得できず、結果として記録情報の解読・再生ができないこととなり、不法複写された（すなわち、識別情報と暗号化鍵情報とが正規に対応付けられない形で複写された）記録情報が再生されることを防止できる。

## 【 0 3 6 3 】

従って、当該記録情報が復号されずに情報記録媒体に記録されている形のままで他の情報記録媒体に不法複写されている場合でも、識別情報と暗号化鍵情報とが正規の対応関係を有さないので、暗号化記録情報の解読のための鍵情報が取得できないこととなり、不法複写された記録情報が再生されることを防止することができる。

## 【図面の簡単な説明】

## 【図 1】

第 1 実施形態のカッティング装置の概要構成を示すブロック図である。

## 【図 2】

第 1 実施形態のカッティング動作を示すフローチャートである。

## 【図 3】

第 1 実施形態のデータにおける ECC ブロックの構造を示す図であり、（a）はデータセクタの構造を示す図であり、（b）は ECC ブロックの構造を示す図である。

## 【図 4】

第 1 実施形態の置換情報挿入後の ECC ブロックの構造を示す図である。

## 【図 5】

第 1 実施形態のデータの物理フォーマットを示す図である。

## 【図 6】

第 1 実施形態の情報記録装置の概要構成を示すブロック図である。

【図 7】

第 1 実施形態の情報再生装置の概要構成を示すブロック図である。

【図 8】

第 1 実施形態の再生動作を示すフローチャートである。

【図 9】

第 2 実施形態のカッティング装置の概要構成を示すブロック図である。

【図 1 0】

第 2 実施形態の置換情報生成器の細部構成を示すブロック図であり、（a）は置換情報生成器の第 1 の形態を示すブロック図であり、（b）は置換情報生成器の第 2 の形態を示すブロック図であり、（c）は置換情報生成器の第 3 の形態を示すブロック図であり、（d）は置換情報生成器の第 4 の形態を示すブロック図であり、（e）は置換情報生成器の第 5 の形態を示すブロック図である。

【図 1 1】

第 2 実施形態の情報記録装置の概要構成を示すブロック図である。

【図 1 2】

第 2 実施形態の情報再生装置の概要構成を示すブロック図である。

【符号の説明】

- 1 … データ生成器
- 2 … E C C エンコーダ
- 3 … 置換情報書込器
- 4 … エンコーダ
- 5 … レーザ発生器
- 6 … 光変調器
- 7 … 対物レンズ
- 8 … 回転サーボ回路
- 9 … 回転検出器
- 1 0 … 送りサーボ回路
- 1 1 … 位置検出器
- 1 2 … 送りユニット

1 3、5 1、6 1…スピンドルモータ  
1 4…レジスト  
1 5…ガラス基板  
1 6…識別情報生成器  
1 7、6 7、7 5、8 1…置換情報生成器  
1 8、7 7…置換情報位置生成器  
2 0…データセクタ  
2 1…I D 情報  
2 2…I D 情報誤り訂正コード  
2 3…予備データ  
2 4、4 1、4 3…データ  
2 5…エラー検出コード 2 5  
3 0、3 0' …E C C ブロック  
3 1…E C C 内符号  
3 2…E C C 外符号  
3 3…データブロック  
3 4…訂正ブロック  
3 5…置換情報  
4 0…レコーディングセクタ  
4 2…シンクフレーム  
5 0、6 0…ピックアップ  
5 2、7 1…サーボ I C  
5 3、7 0…システムコントローラ  
5 4…ストラテジ回路  
6 2…R F アンプ  
6 3…デコーダ  
6 4…置換情報抽出器  
6 5…エラー訂正回路  
6 6…出力制御器

6 8 … 識別情報抽出器

6 9 … 識別情報比較器

7 6 … データ暗号化器

7 8 … 鍵情報生成器

8 2 … 置換情報復号器

9 5、9 8 … 暗号化器

9 6 … 加算器

9 7 … 関数化器

1 0 0 … DVD

C 1、C 2 … カッティング装置

R 1、R 2 … 情報記録装置

S 1、S 2 … 情報再生装置

B … 光ビーム

H、H' … ヘッダ

S d … データ信号

S d e … 付加データ信号

S d r … 置換データ信号

S r … 記録データ信号

S c g、S c g' … 置換情報

S p o … 位置情報

S i d、S i d p … 識別情報

S r s … 記録信号

S c i、S c s、S c s p、S c p、S c p p、S p u … 制御信号

S s p、S s p p … ピックアップ制御信号

S s s、S s s p … スピンドル制御信号

S p … 検出信号

S r f … R F 信号

S d c … 再生信号

S c r … エラー訂正信号

S out…出力信号

S k…鍵情報

S ad…暗号化データ信号

S ks、S kss…暗号化鍵情報

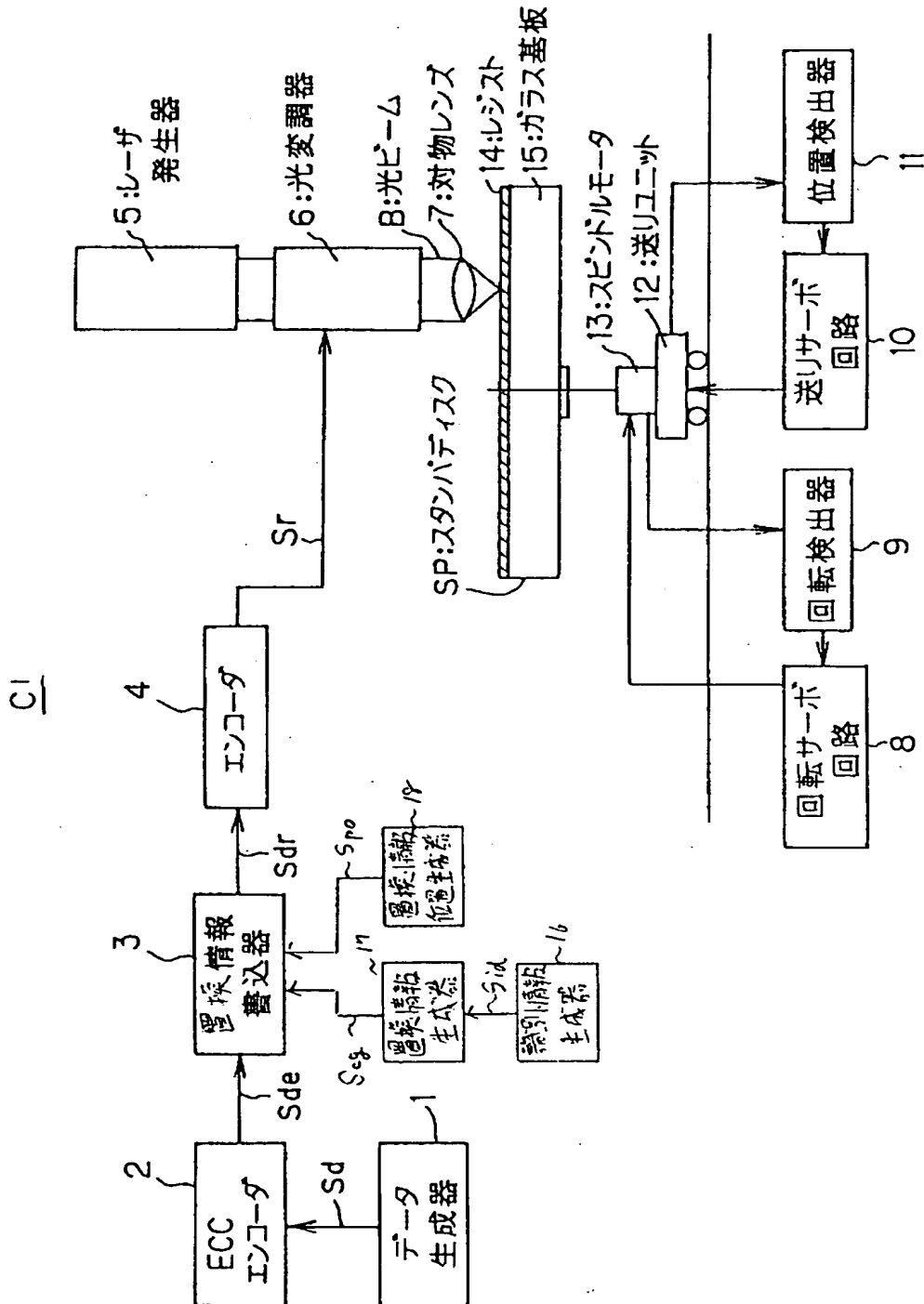
S did…暗号化識別情報

S fid…関数化識別情報

【書類名】 図面

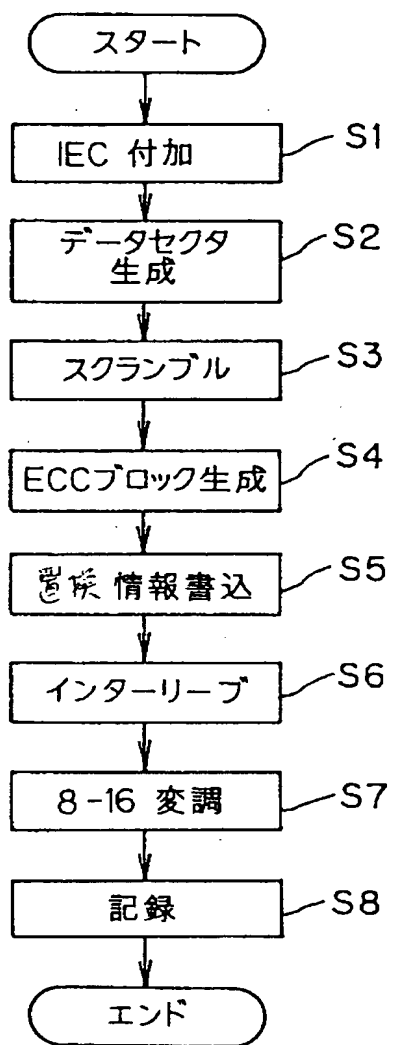
【図 1】

第 1 実施形態のカッティング装置の概要構成を示すブロック図



【図 2】

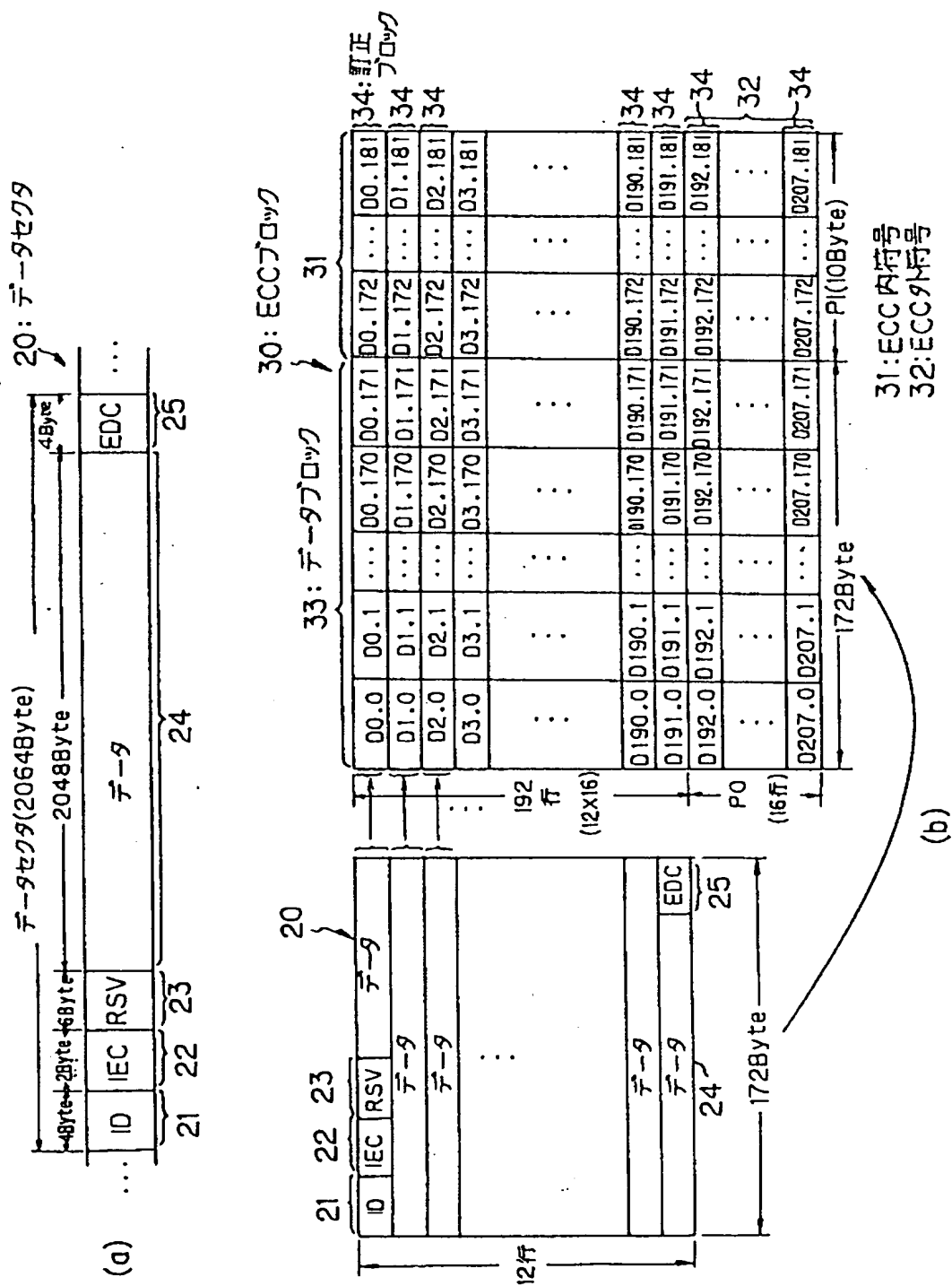
第 1 実施形態のカッティング動作を示すフローチャート





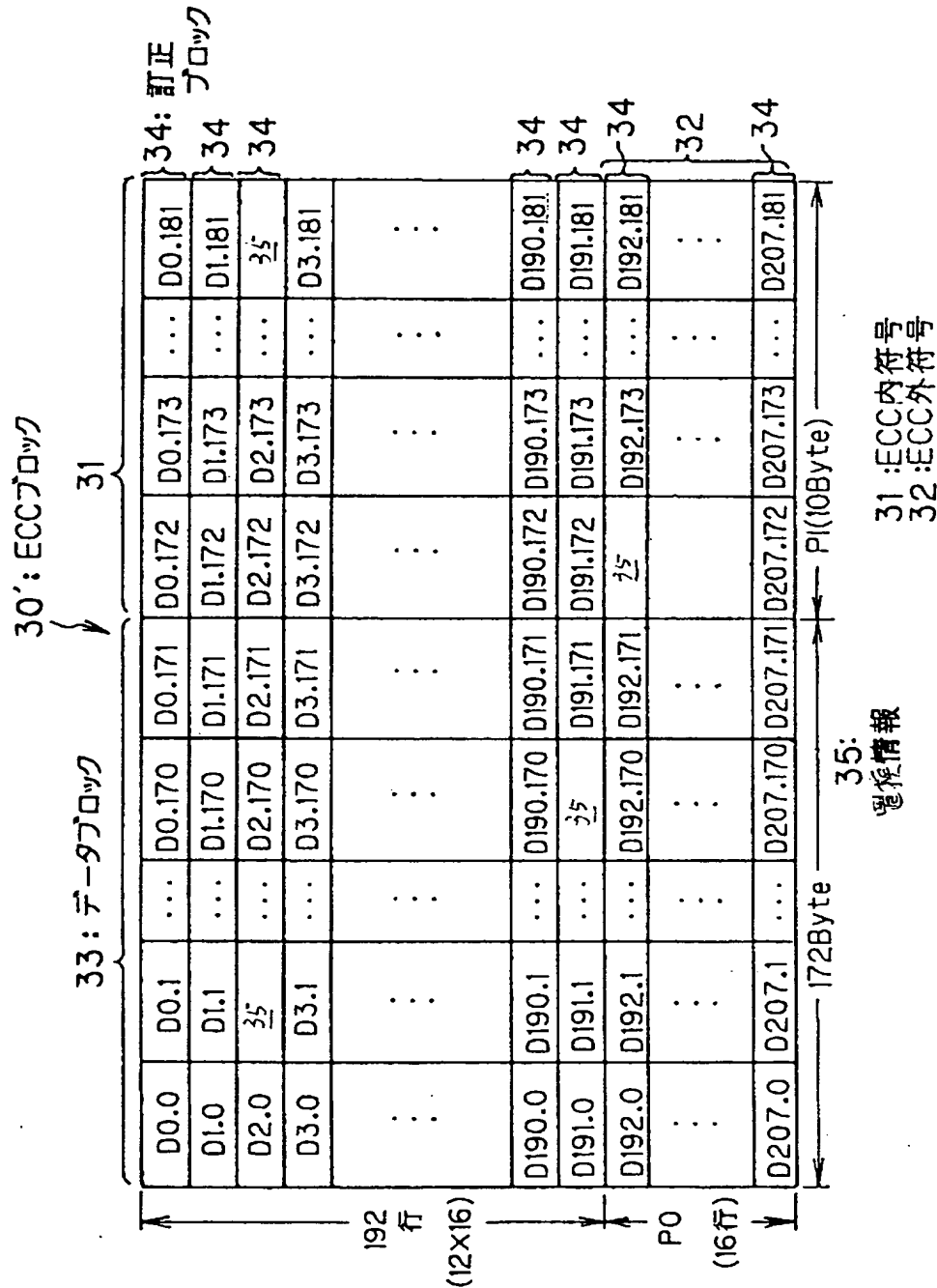
【図 3】

## 第 1 実施形態のデータにおける ECC ブロックの構造



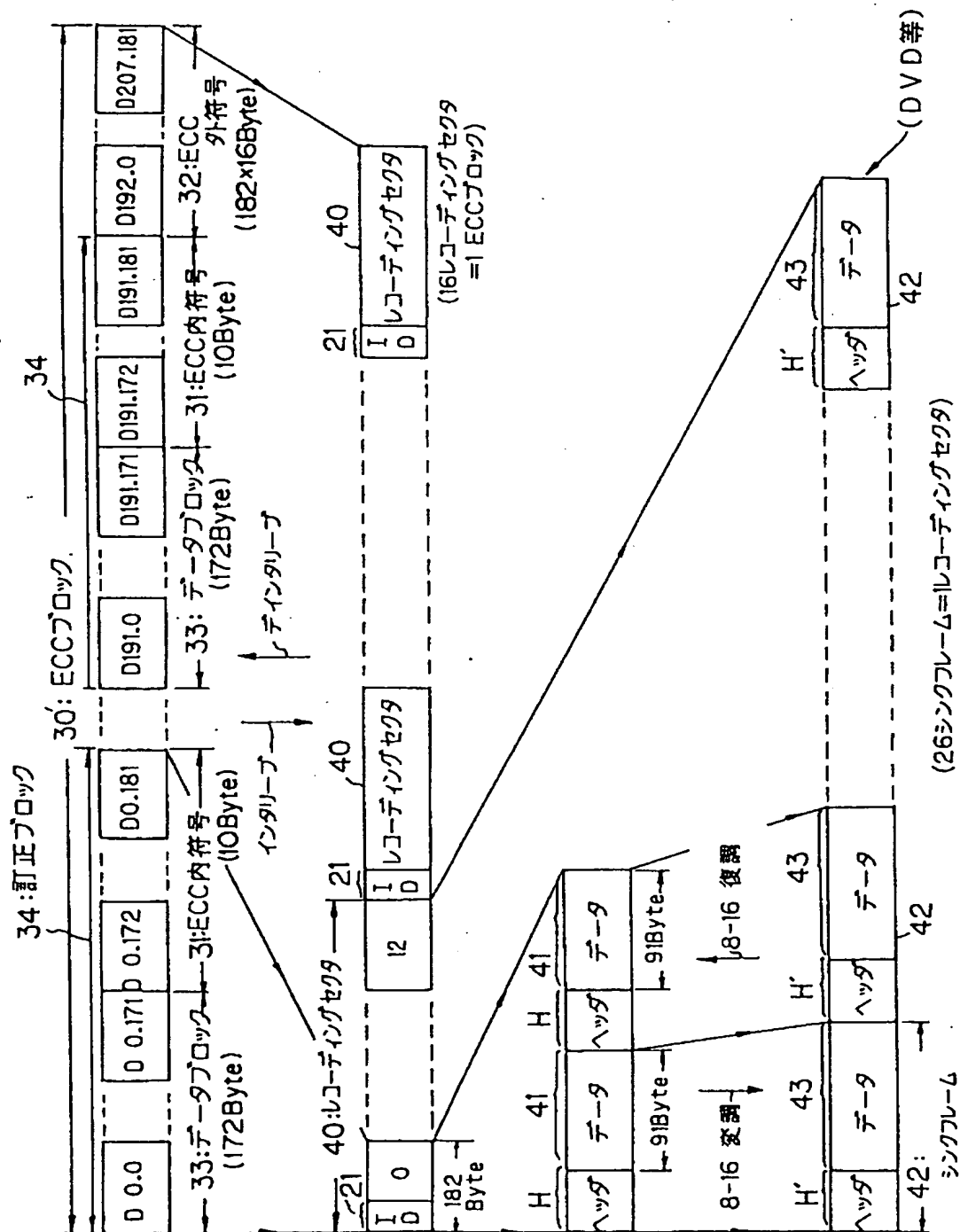
【図 4】

第 1 実施形態の符号情報挿入後の ECC ブロックの構造



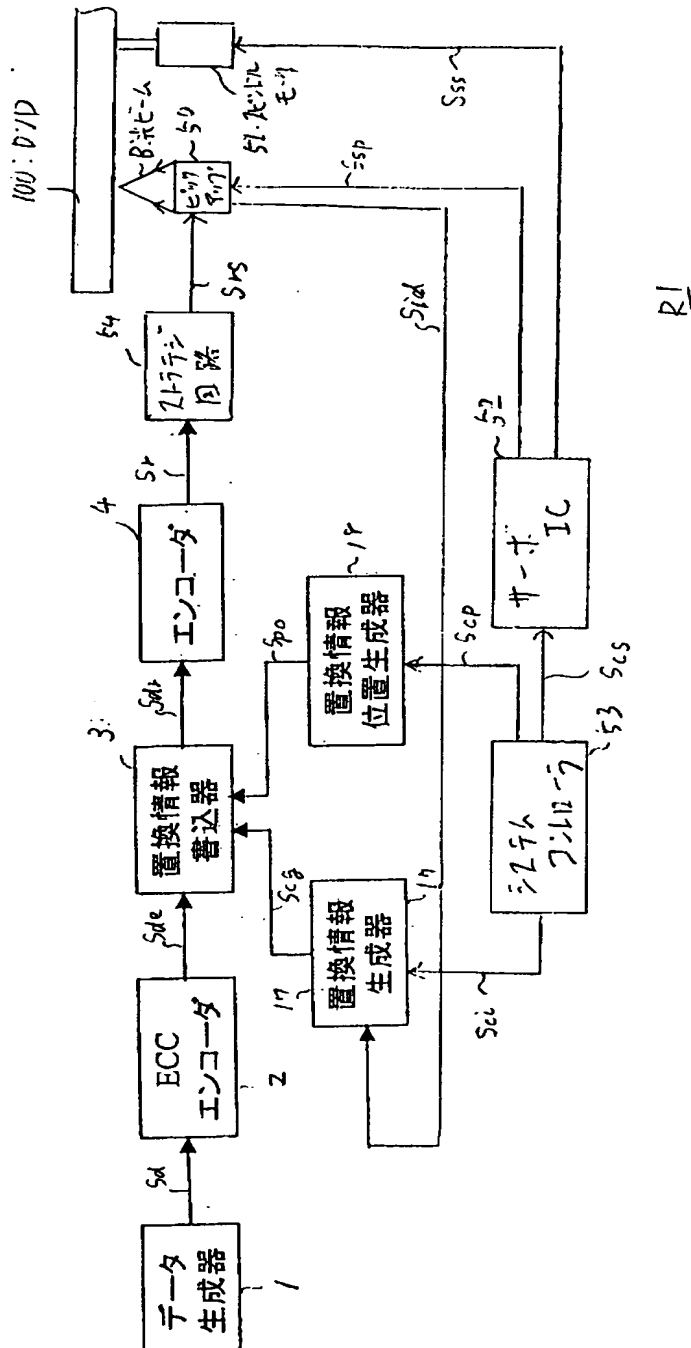
【図 5】

第 1 実施形態のデータの物理フォーマット



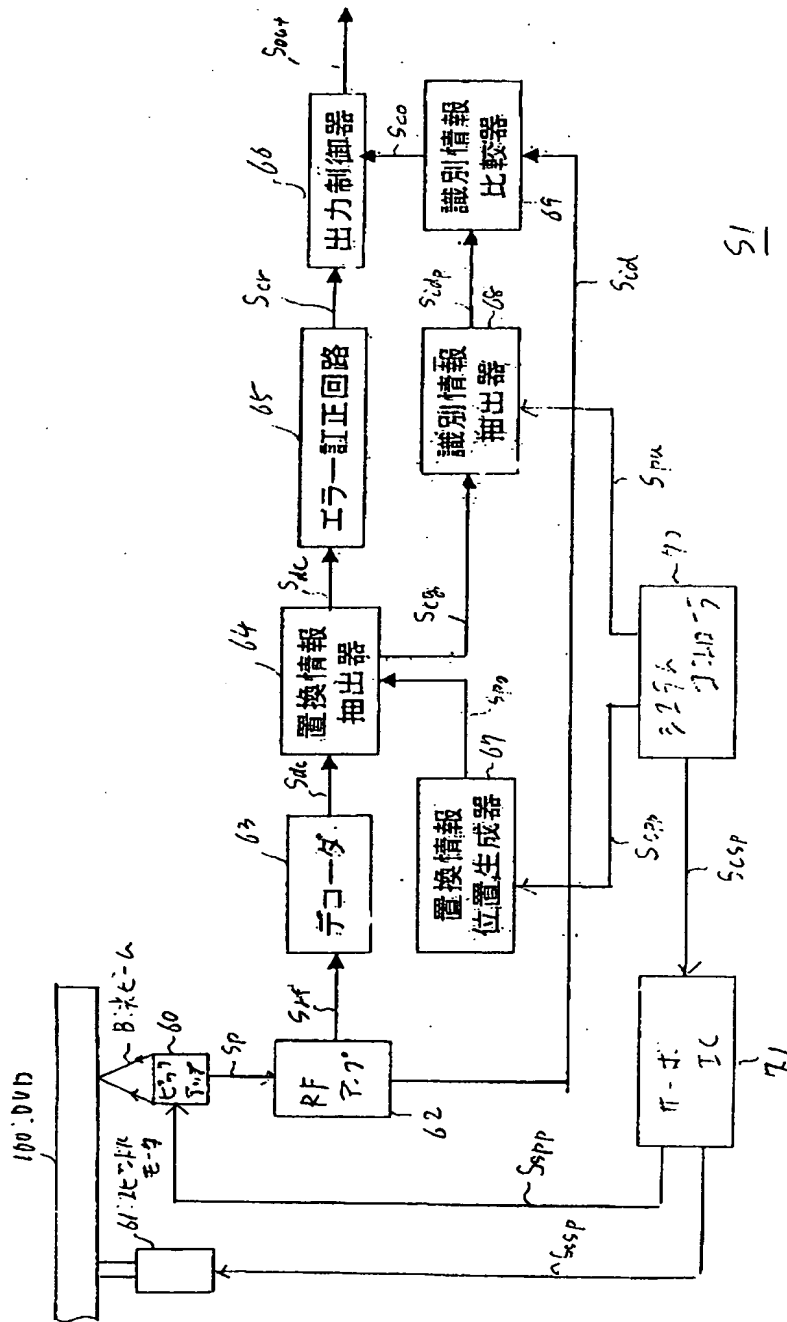
【图 6】

### 第1実施形態の情報記録装置の概要構成を示すブロック図



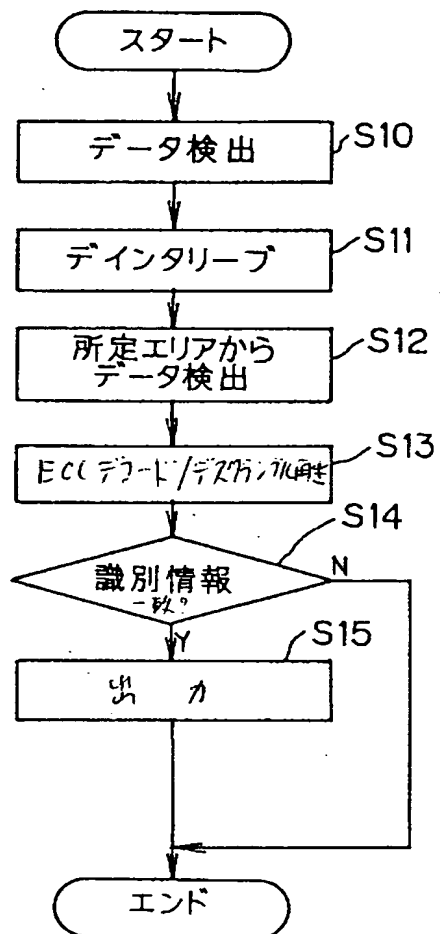
【図7】

第1実施形態の情報再生装置の概要構成を示すブロック図



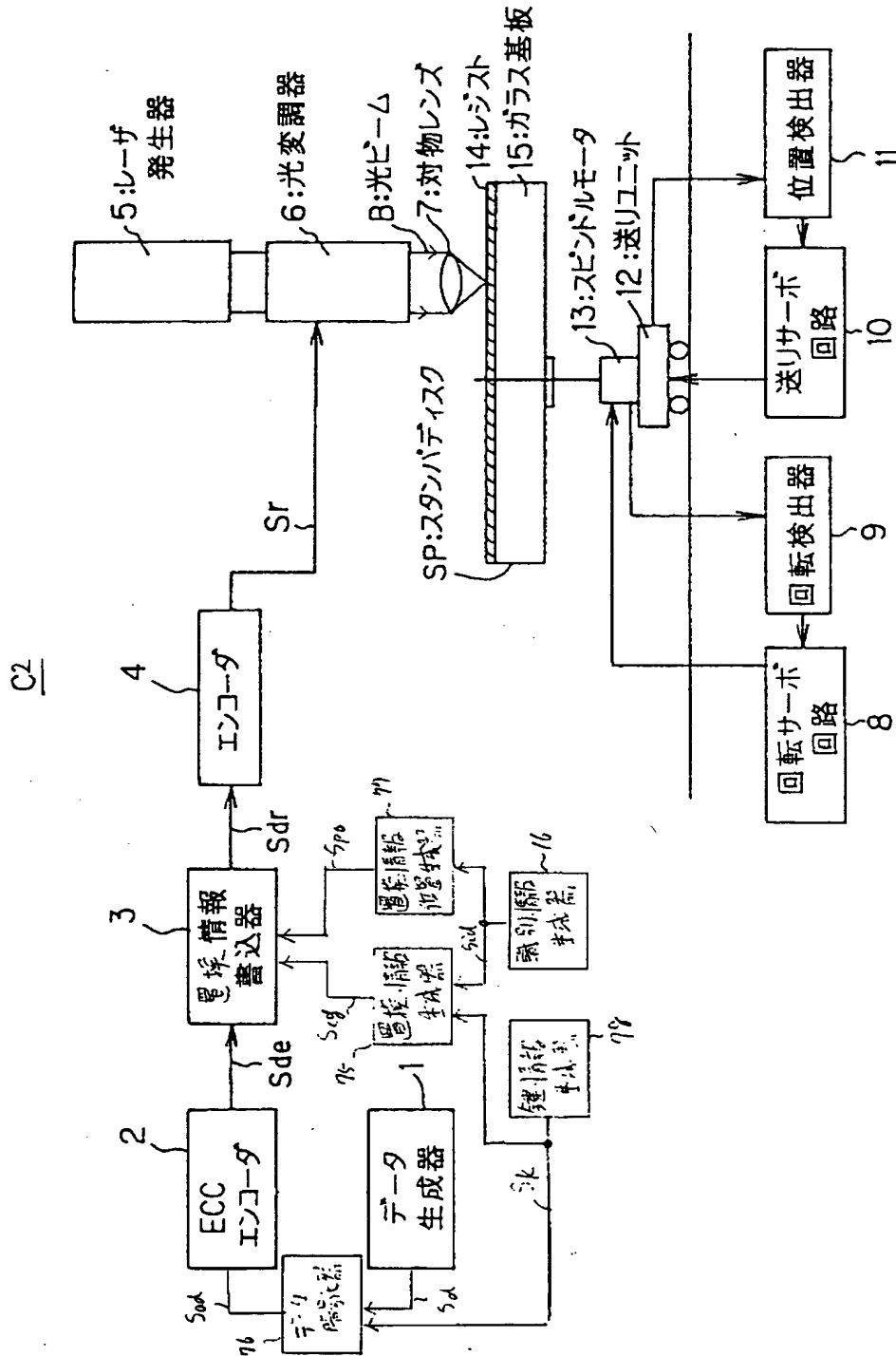
【図 8】

第 1 実施形態の再生動作を示すフローチャート



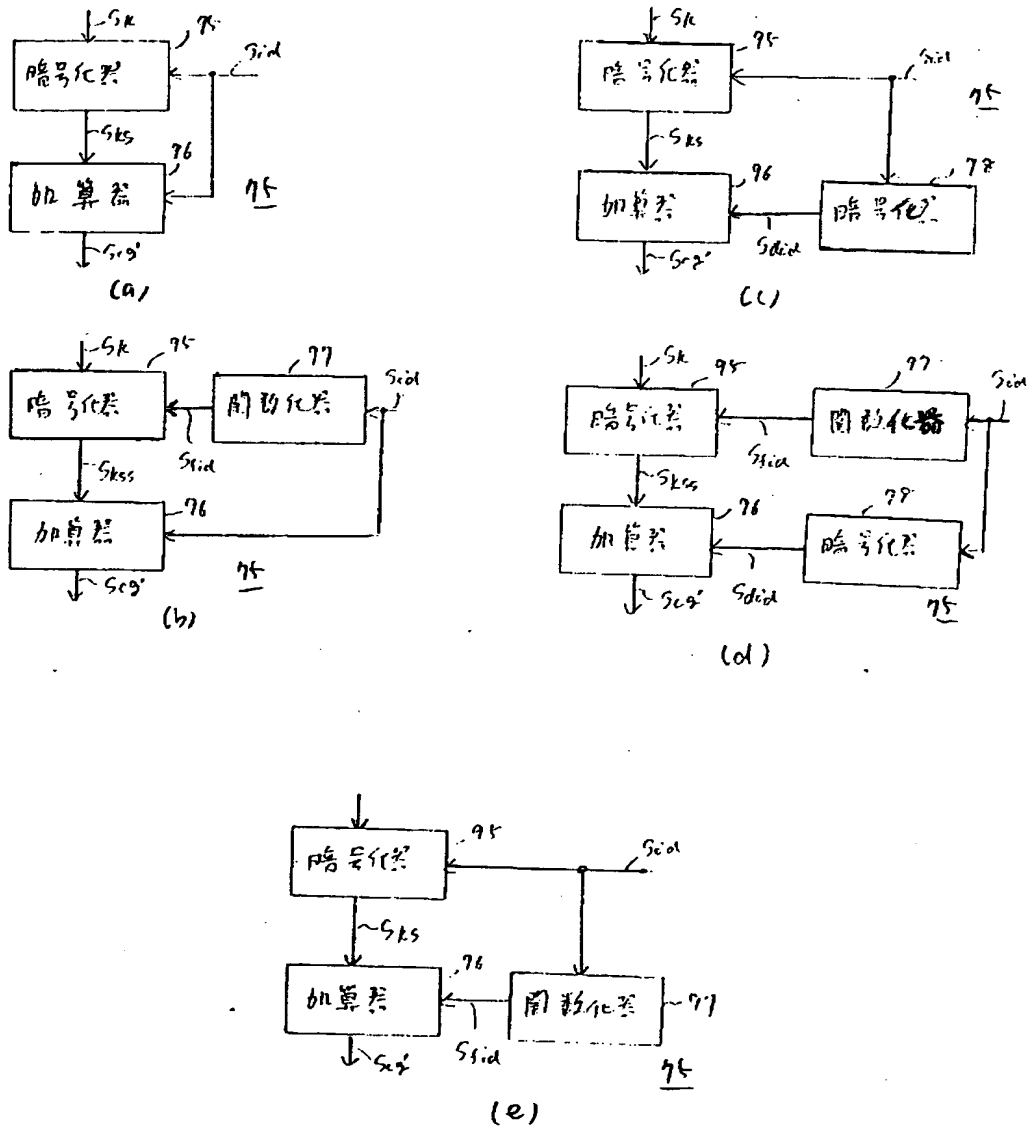
【图 9】

第2実施形態のカッティング装置を概要構成を示すブロック図



【図10】

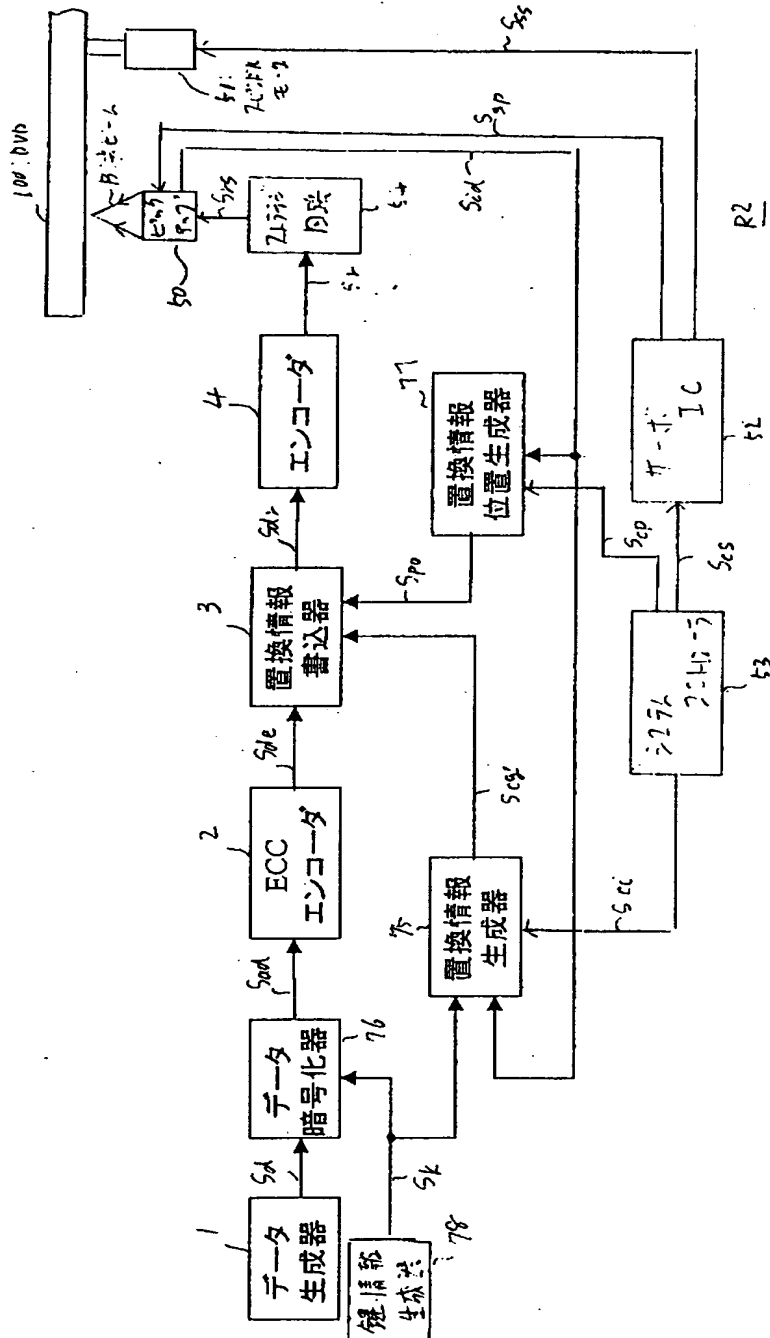
第2実施形態の置換情報生成器の細部構成を示すブロック図





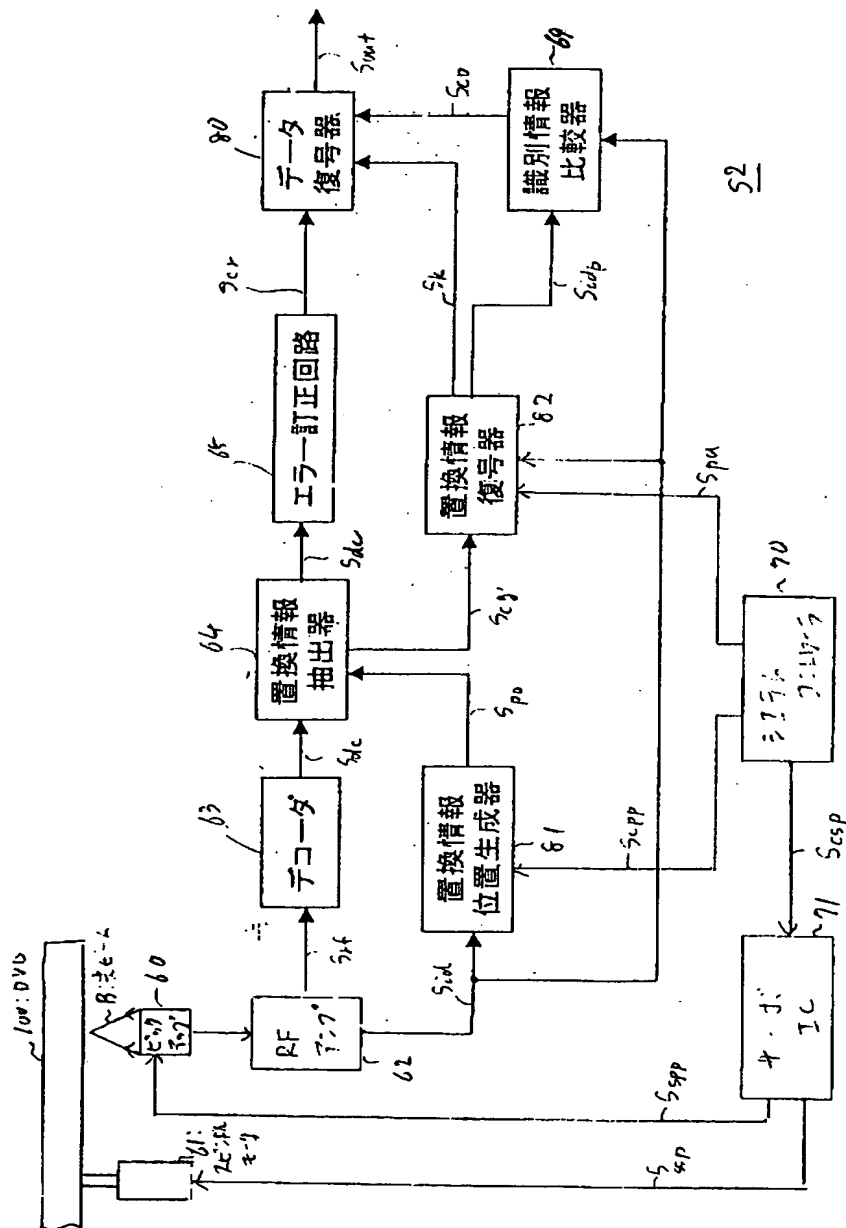
【図 1 1】

## 第2実施形態の情報記録装置の概要構成を示すブロック図



【图 12】

## 第2実施形態の情報再生装置の概要構成を示すブロック図



【書類名】 要約書

【要約】

【課題】 記録情報が復号されずに記録されている形のままで他の情報記録媒体に不法複写された場合でも、当該不法複写された記録情報が再生されることを防止することが可能な情報記録装置等を提供する。

【解決手段】 本発明に係るカッティング装置 C 1 は、記録情報を記録すべき DVD 個々に固有の識別情報 S i d を用いて置換情報 S c g を生成する置換情報生成器 1 7 と、記録情報の一部を生成された置換情報 S c g に置換し置換データ信号 S d r を生成する置換情報書込器 3 と、生成された置換データ信号 S d r を、置換情報 S c g の生成に用いられた識別情報 S i d に対応する DVD に記録する光変調器 6 と、を備える。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005016]

1. 変更年月日 1990年 8月31日  
[変更理由] 新規登録  
住 所 東京都目黒区目黒1丁目4番1号  
氏 名 パイオニア株式会社